ADSS Web RA Server

Microsoft Intune SCEP

Deployment Guide

ASCERTIA LTD

JANUARY 2024

DOCUMENT VERSION- 1.0.4

This document contains commercial-in-confidence material. It must not be disclosed to any third party without the written authority of Ascertia Limited.

Document Revisions				
Version	**Date**	**Author**	**Action**	**Notes**
1.0.0	15 Sep 23	HS	Created	Initial draft
1.0.1	18 Sep 23	HS	Reviewed	Revisions in text
1.0.2	22 Sep 23	HS	Updated	Updated after QA's review
1.0.3	17 Oct 23	HS	Updated	Rearranged structure after PO's feedback
1.0.4	5 Jan 23	HS	Updated	Restructure content sequence

CONTENTS

1 Introduction

This manual is intended for ADSS Web RA Server administrators responsible for installation and configurations of the Windows Certificate Enrolment. It describes an end-to-end flow, right from installation, to configurations and certificate issuance. It is assumed that the reader has a basic knowledge of digital signatures, certificates and information security.

1.1 Scope

This manual describes how to install and configure Ascertia ADSS Web RA Server and Microsoft Intune SCEP service to enable certificate issuance of digital certificates.

1.2 Intended Readership

This manual is intended for use by Ascertia staff and customers who will be installing and configuring ADSS Server and ADSS Web RA Server to issue certificates within a Microsoft Intune admin centre. It is assumed that the reader has a basic knowledge of standard PKI commands.

1.3 Conventions

The following typographical conventions are used in this guide to help locate and identify information:

- Bold text identifies menu names, menu options, items that can be clicked on the screen, file names, folder names, and keyboard keys.
- `Courier New` font identifies code and text that appears on the command line.
- **`Bold Courier New`** identifies commands that are required to be typed in.

1.4 Technical Support

If Technical Support is required, Ascertia has a dedicated support team. Ascertia Support can be reached/accessed in the following ways:

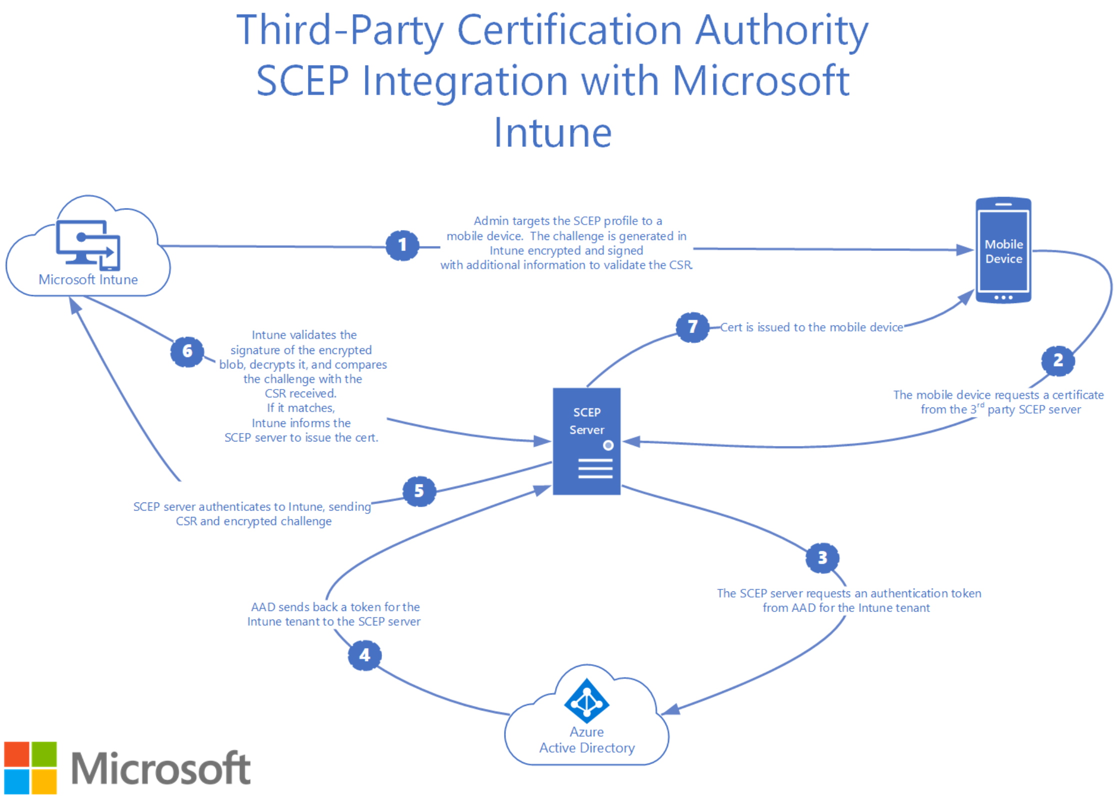
Website	https://www.ascertia.com
Email	support@ascertia.com
Knowledge Base	https://www.ascertia.com/products/knowledge-base/adss-server/
FAQs	https://ascertia.force.com/partners/login

In addition to the free support services detailed above, Ascertia provides formal support agreements with all product sales. Please contact sales@ascertia.com for more details.

When sending support queries to Ascertia Support team send ADSS Trust Monitor logs. Use the Ascertia's trace log export utility to collect logs for last two days or from the date, the problem arose. It will help the support team to diagnose the issue faster. Follow the instructions on how to run the trace log export utility.

2 Microsoft Intune

Microsoft Intune is a cloud-based endpoint management solution. It manages user access and simplifies application and device management across various devices, including mobile devices, desktop computers, and virtual endpoints. Microsoft Intune can help you keep your managed devices secure and up to date while helping you to protect your organization’s data from compromised devices.



Third-Party Certification Authority SCEP Integration with Microsoft Intune

1 Admin targets the SCEP profile to a mobile device. The challenge is generated in Intune encrypted and signed with additional information to validate the CSR.

2 The mobile device requests a certificate from the 3rd party SCEP server

3 The SCEP server requests an authentication token from AAD for the Intune tenant

4 AAD sends back a token for the Intune tenant to the SCEP server

5 SCEP server authenticates to Intune, sending CSR and encrypted challenge

6 Intune validates the signature of the encrypted blob, decrypts it, and compares the challenge with the CSR received. If it matches, Intune informs the SCEP server to issue the cert.

7 Cert is issued to the mobile device

2.1. Microsoft Intune SCEP

Intune enables the utilization of the Simple Certificate Enrollment Protocol (SCEP) for authenticating connections to both your applications and corporate resources. SCEP relies on the Certification Authority (CA) certificate to ensure the security of the communication when generating the Certificate Signing Request (CSR). If your infrastructure is compatible with SCEP, you can utilize Intune SCEP certificate profiles, which are a specific type of device profile within Intune, for distributing these certificates to your devices.

Limitations with respect to MS Intune:

Since Ascertia is still using the free version, consider the following points before you begin.

- Log out from official Ascertia MS office account before performing any configurations.
- Use different MS office credentials to sign-up to MS Intune and MS Azure Portal.
- Ensure they are not connected to Ascertia's internet when creating/working on Groups in MS Intune.

- Sometimes, VPN may also affect some things to work with MS Intune; you may want to turn it off.

3 Deployment Pre-Requisites

The installation of ADSS Web RA Server to support Microsoft Intune SCEP requires the following pre-requisites to be met.

Installation of:

- ADSS Server installed with Root and Issuing CA pre-configured
- SMTP Server
- Microsoft Azure Active Directory

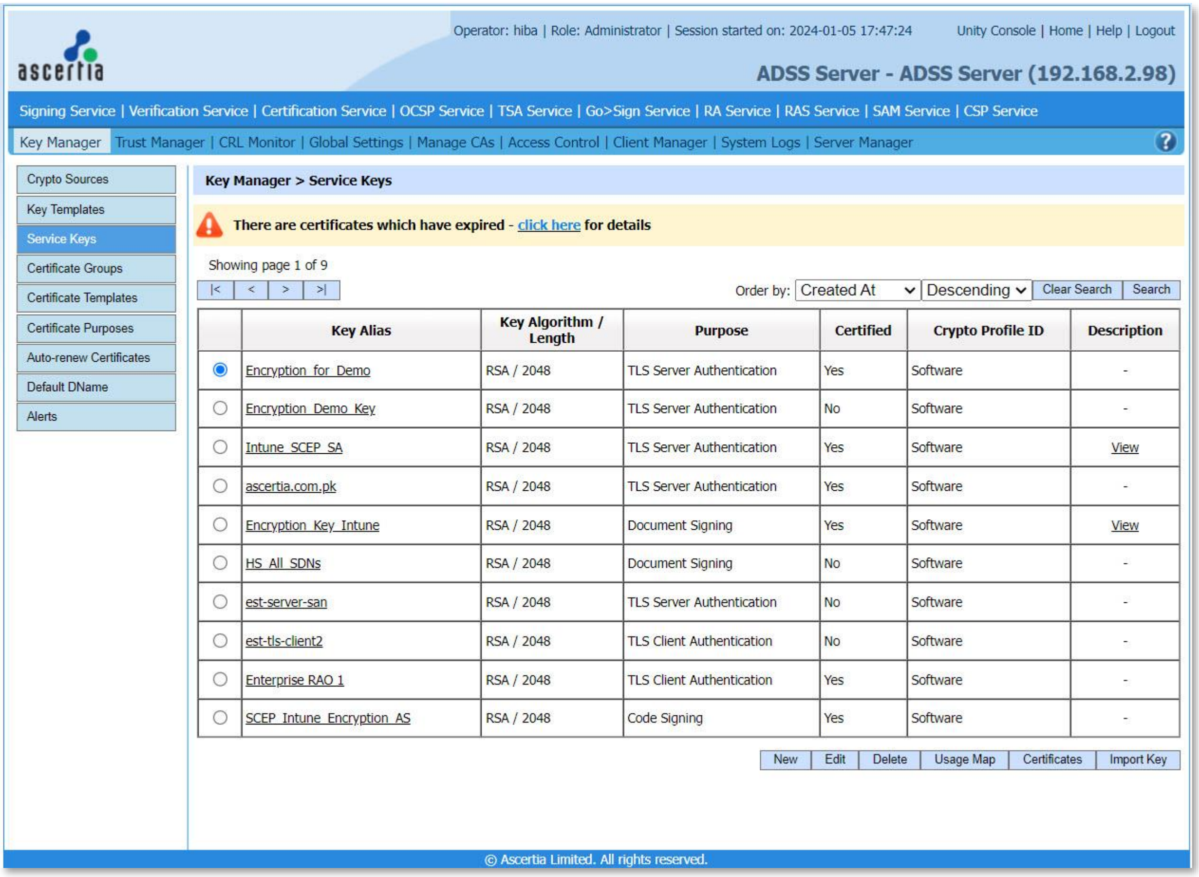
3.1. ADSS Server Pre-Requisites

Before you begin with Microsoft Intune setup, ADSS Server must be installed and configured. A Root and Issuing Certification Authority need to be created prior to installing the ADSS Web RA Server. The Issuing CA operator will need to create certification profiles required to issue certificates to Android, iOS and Windows platforms.

You are required to upload Root and Intermediate certificates, but if you do not have them, the steps below will guide to create certificates from ADSS Server to build a chain of trusted certificates, that will be required while creating configuration profiles in the Microsoft Intune admin center.

3.1.1 Generate a Key Pair from ADSS Server

1. Access the ADSS Server. From the main menu, click the Key Manager > Service Keys.
2. To generate a new key press the New button in the main Service Keys page.


ascertia
Operator: hiba | Role: Administrator | Session started on: 2024-01-05 17:47:24
Unity Console | Home | Help | Logout
ADSS Server - ADSS Server (192.168.2.98)
Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager
Crypto Sources
Key Templates
Service Keys
Certificate Groups
Certificate Templates
Certificate Purposes
Auto-renew Certificates
Default DName
Alerts
|< < > >|
Order by: Created At Descending Clear Search Search
New Edit Delete Usage Map Certificates Import Key
© Ascertia Limited. All rights reserved.

Key Manager > Service Keys

There are certificates which have expired - click here for details

Showing page 1 of 9

	Key Alias	Key Algorithm / Length	Purpose	Certified	Crypto Profile ID	Description
●	Encryption_for_Demo	RSA / 2048	TLS Server Authentication	Yes	Software	-
○	Encryption_Demo_Key	RSA / 2048	TLS Server Authentication	No	Software	-
○	Intune_SCEP_SA	RSA / 2048	TLS Server Authentication	Yes	Software	View
○	ascertia.com.pk	RSA / 2048	TLS Server Authentication	Yes	Software	-
○	Encryption_Key_Intune	RSA / 2048	Document Signing	Yes	Software	View
○	HS_All_SDNs	RSA / 2048	Document Signing	No	Software	-
○	est-server-san	RSA / 2048	TLS Server Authentication	No	Software	-
○	est-tls-client2	RSA / 2048	TLS Client Authentication	No	Software	-
○	Enterprise RAO 1	RSA / 2048	TLS Client Authentication	Yes	Software	-
○	SCEP_Intune_Encryption_AS	RSA / 2048	Code Signing	Yes	Software	-

A form is presented. The ones with a red Asterisk are mandatory fields:

- Key Alias

Define a name for the new key e.g. Encryption_for_Demo.

- Purpose

Select the certificate purpose for this key pair e.g. TLS Server Authentication.

- Crypto Profile

Select where to generate and store this key e.g. Software.

- Key Algorithm

Select the key algorithm to be used e.g. RSA.

- Key Length

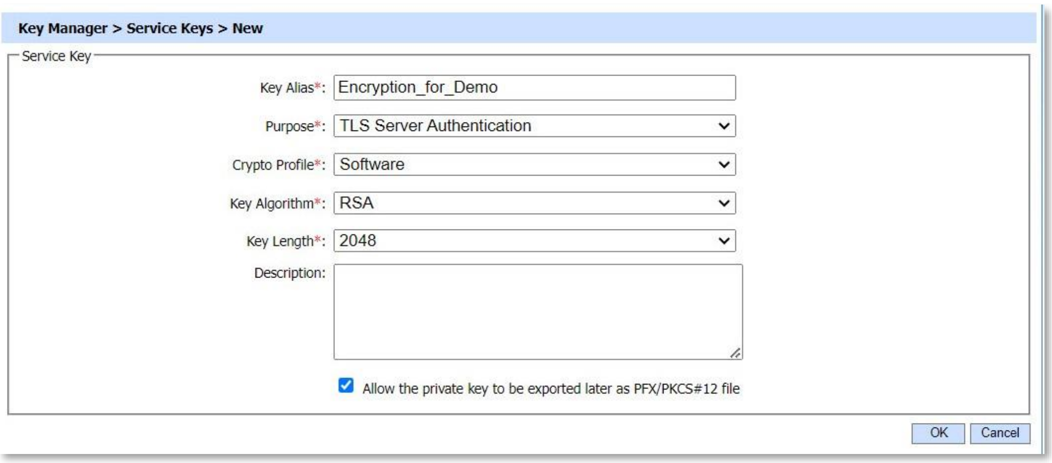
Select the key length to be used e.g. 2048.

- Description

Enter a description.

- Select Allow the private key to be exported later

Then click OK.



Key Manager > Service Keys > New

Service Key

Key Alias*: Encryption_for_Demo

Purpose*: TLS Server Authentication

Crypto Profile*: Software

Key Algorithm*: RSA

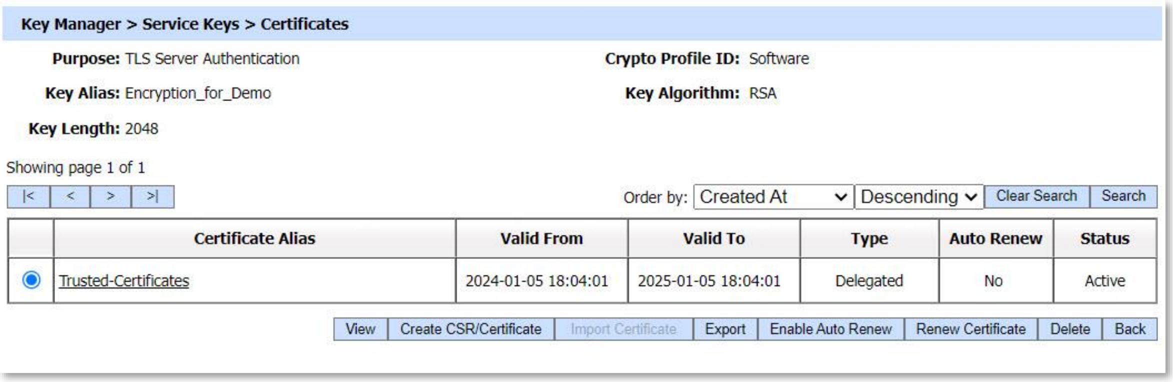
Key Length*: 2048

Description:

☑ Allow the private key to be exported later as PFX/PKCS#12 file

3.1.2 Create a Certificate in ADSS Server

1. Click on the key pair you created above, e.g. Encryption_for_Demo, then click Create CSR/Certificate



Key Manager > Service Keys > Certificates

Purpose: TLS Server Authentication

Crypto Profile ID: Software

Key Alias: Encryption_for_Demo

Key Algorithm: RSA

Key Length: 2048

Showing page 1 of 1

Order by: Created At, Descending

	Certificate Alias	Valid From	Valid To	Type	Auto Renew	Status
●	Trusted-Certificates	2024-01-05 18:04:01	2025-01-05 18:04:01	Delegated	No	Active

2. In the General Details section: (The ones with a red steric are mandatory fields)

- Certificate Alias

Define a unique name for the certificate e.g. Trusted-Certificate.

3. In the Requested Certificate Details section, enter the Subject Distinguished Name (SDNs):

- Common Name

Enter a common e.g. ADSS_Sample_Demo.

- The rest of the fields are optional include the Given Name, Surname, Title, Organization Unit, Organization, Organization Identifier, Email, Locality, Street Address, Postal Code, State, Country, Serial Number, Business Category.

To learn more about the description of these fields, you can refer to ADSS Server Admin Guide.

4. The following fields appear under the Subject alternative Name Details. (These fields are not mandatory to be filled)

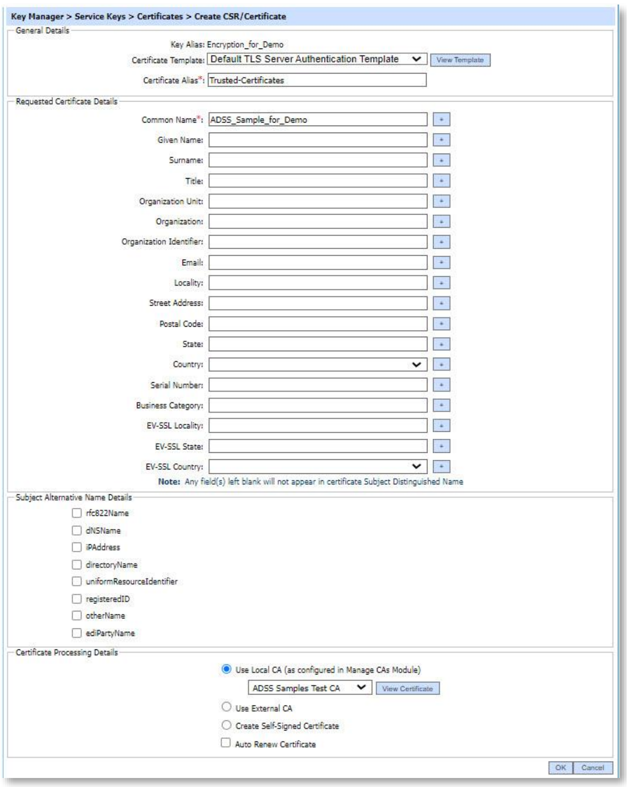
Rfc822Name, dNSName, iPAddress, directoryName, uniformResourceIdentified, registeredID, otherName, ediPartyName.

5. In the Certificate Processing Details section

- Select Use Local CA (as configured in manage CAs Module)

From the drop down, select the certificate e.g. ADSS_Sample_for_Demo, and click OK.

In this case, Key Manager will automatically communicate with the ADSS Local CA and the certificate will be issued and imported within Key Manager without further manual intervention.



Key Manager > Service Keys > Certificates > Create CSR/Certificate

General Details

Key Alias: Encryption_for_Demo

Certificate Template: Default TLS Server Authentication Template

Certificate Alias*: Trusted-Certificates

Requested Certificate Details

Common Name*:	ADSS_Sample_for_Demo
Given Name:	
Surname:	
Title:	
Organization Unit:	
Organization:	
Organization Identifier:	
Email:	
Locality:	
Street Address:	
Postal Code:	
State:	
Country:	
Serial Number:	
Business Category:	
EV-SSL Locality:	
EV-SSL State:	
EV-SSL Country:	

Note: Any field(s) left blank will not appear in certificate Subject Distinguished Name

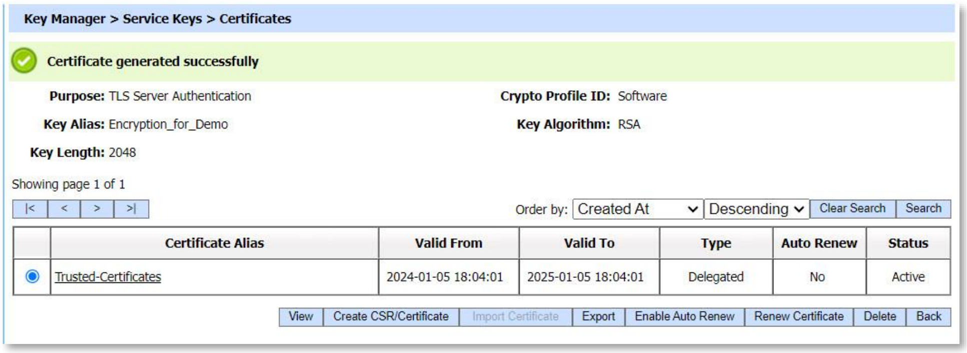
Subject Alternative Name Details

- □ rfc822Name
- □ dNSName
- □ iPAddress
- □ directoryName
- □ uniformResourceIdentifier
- □ registeredID
- □ otherName
- □ ediPartyName

Certificate Processing Details

- ● Use Local CA (as configured in Manage CAs Module)
  - ADSS Samples Test CA
- ○ Use External CA
- ○ Create Self-Signed Certificate
- □ Auto Renew Certificate

The certificate will be generated.



Key Manager > Service Keys > Certificates

Certificate generated successfully

Purpose: TLS Server Authentication

Crypto Profile ID: Software

Key Alias: Encryption_for_Demo

Key Algorithm: RSA

Key Length: 2048

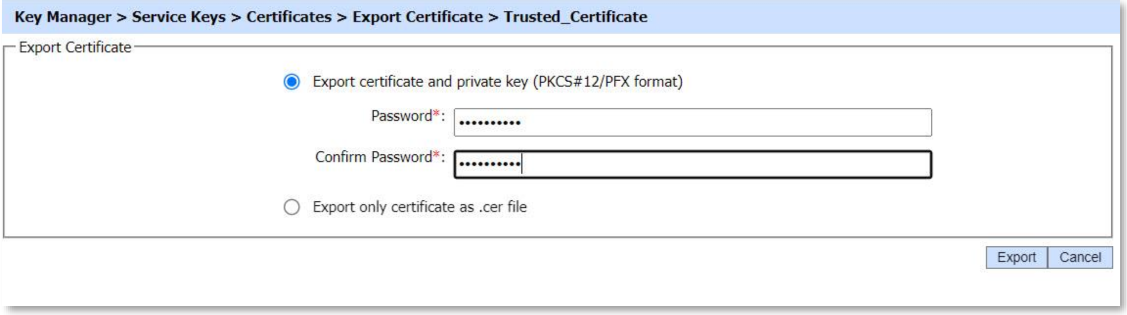
Showing page 1 of 1

Order by: Created At, Descending

	Certificate Alias	Valid From	Valid To	Type	Auto Renew	Status
●	Trusted-Certificates	2024-01-05 18:04:01	2025-01-05 18:04:01	Delegated	No	Active

6. To export a private key and its associated certificate, click the Export button in the Certificates screen. The following form is presented.

- You can choose to export certificate and private key, for which you will be required to enter a password to protect the keys. Then click Export.



Key Manager > Service Keys > Certificates > Export Certificate > Trusted_Certificate

Export Certificate

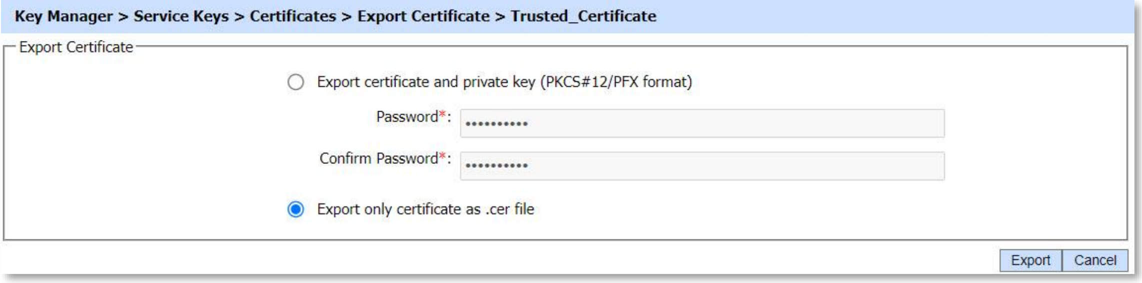
● Export certificate and private key (PKCS#12/PFX format)

Password*: ••••••••••

Confirm Password*: ••••••••••

○ Export only certificate as .cer file

- You can export the certificate as a .CER file, and then click Export.



Key Manager > Service Keys > Certificates > Export Certificate > Trusted_Certificate

Export Certificate

○ Export certificate and private key (PKCS#12/PFX format)

Password*: ••••••••••

Confirm Password*: ••••••••••

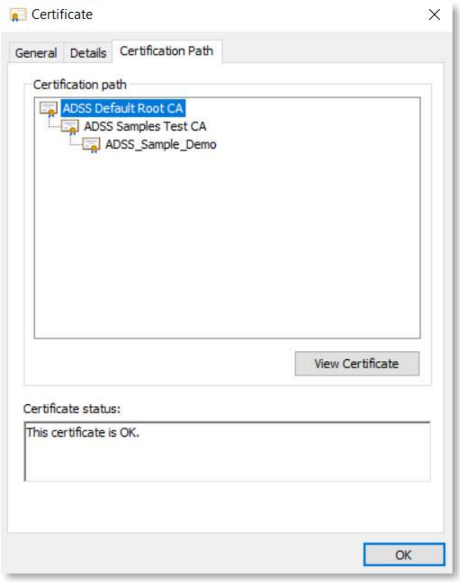
● Export only certificate as .cer file

To build a trust on your deployment machine follow the steps below:

First, you will extract the chain of certificates (Root CA and Intermediate) from the certificate you created from the ADSS Server.

3.1.3 Extract the Root CA Certificate

1. Double-click on your certificate > Open file > Certification Path. Then click View Certificate against the ADSS Default Root CA.



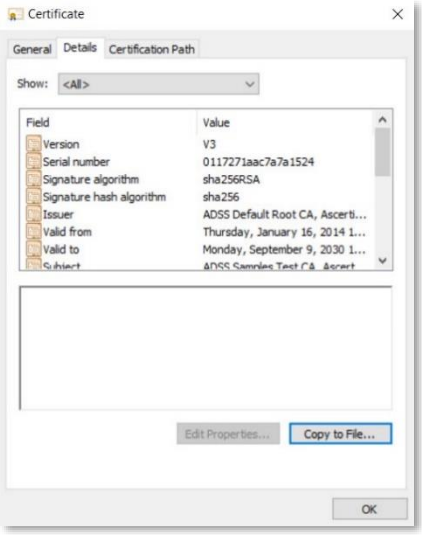
Certification path

ADSS Default Root CA
ADSS Samples Test CA
ADSS_Sample_Demo

Certificate status:

This certificate is OK.

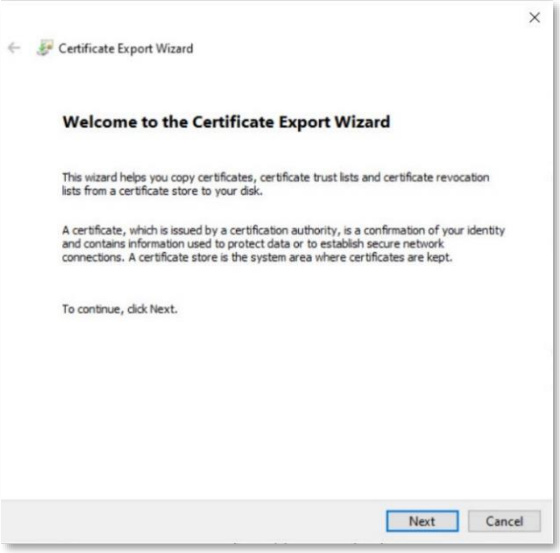
2. From the Details tab click Copy to File…



Show: <All>

Field	Value
Version	V3
Serial number	0117271aac7a7a1524
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADSS Default Root CA, Ascerti...
Valid from	Thursday, January 16, 2014 1...
Valid to	Monday, September 9, 2030 1...
Subject	ADSS Samples Test CA, Ascert...

3. On the Certificate Import Wizard, click Next.



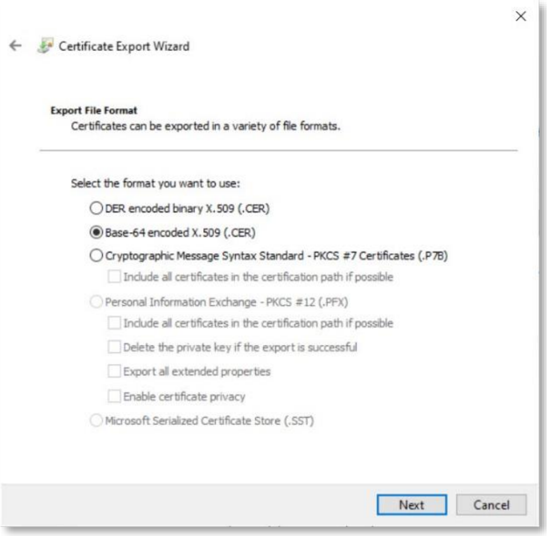
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4. Select the export file format as Base-64 encoded X.509 (.CER) and click Next.

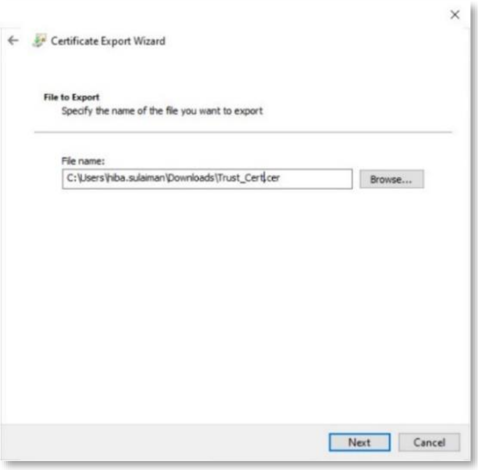


Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ● Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
  - □ Enable certificate privacy
- ○ Microsoft Serialized Certificate Store (.SST)

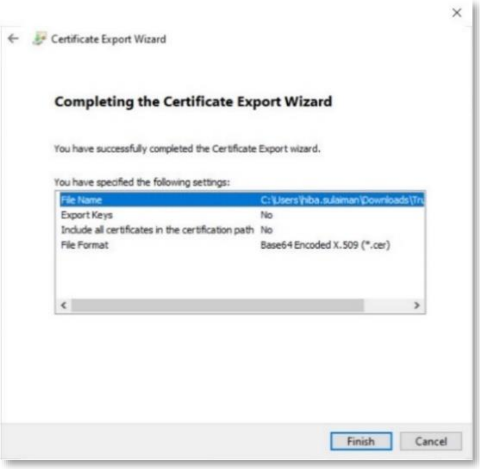
5. In the next step, specify the name of the file you want to export e.g. Trust_Cert and click Next.



File to Export
Specify the name of the file you want to export

File name: C:\Users\hiba.sulaiman\Downloads\Trust_Cert.cer

6. Click Finish to complete the certificate export wizard.



Completing the Certificate Export Wizard

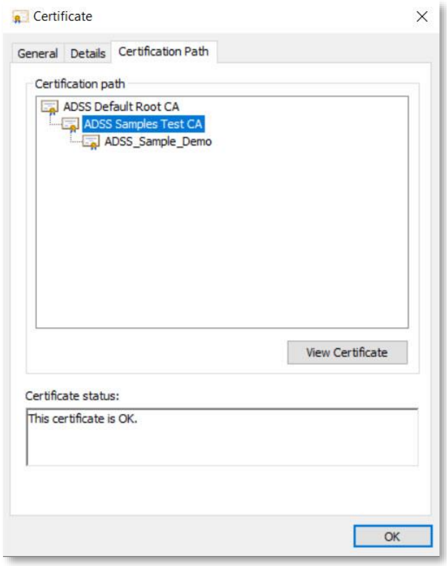
You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\hiba.sulaiman\Downloads\Tru
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

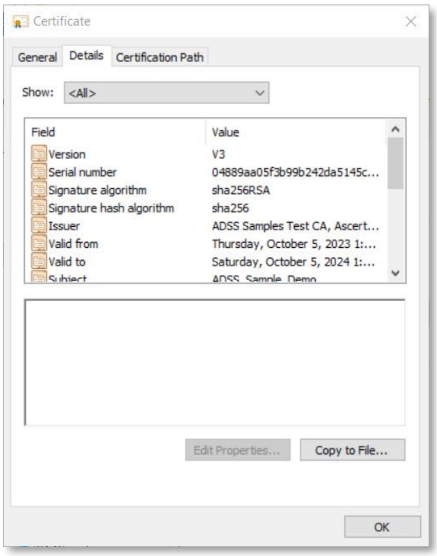
3.1.4 Extract the Intermediate certificate

1. In the next step, you will extract the intermediate certificate from the Trusted_Root. Double-click on your certificate > Open file > Certification Path. Then click View Certificate against the ADSS Samples Test CA.



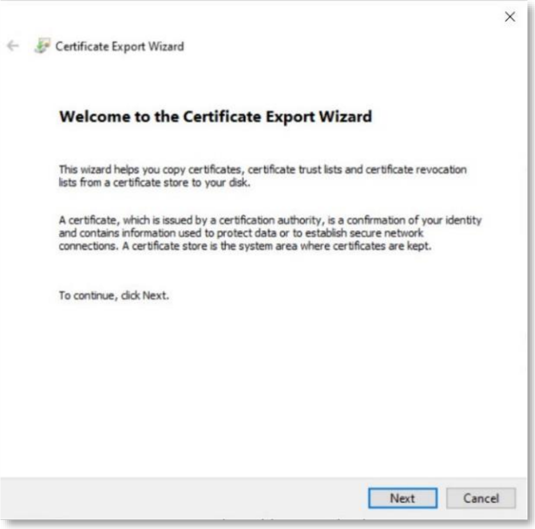
Certificate status:
This certificate is OK.

2. From the Details tab click Copy to File…



Field	Value
Version	V3
Serial number	04889aa05f3b99b242da5145c…
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADSS Samples Test CA, Ascert…
Valid from	Thursday, October 5, 2023 1:…
Valid to	Saturday, October 5, 2024 1:…
Subject	ADSS Sample Demo

3. On the Certificate Import Wizard, click Next.



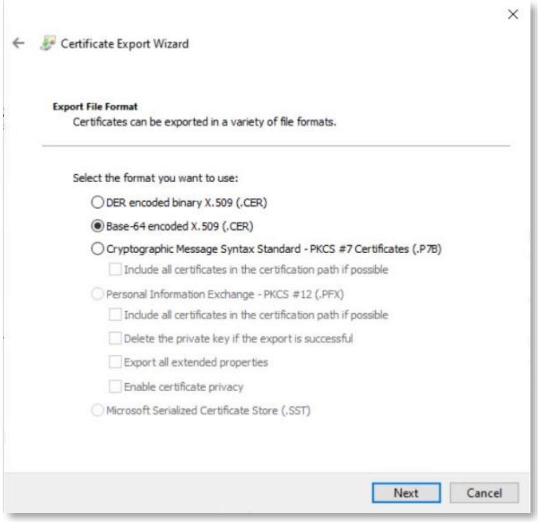
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4. Select the export file format as Base-64 encoded X.509 (.CER) and click Next.

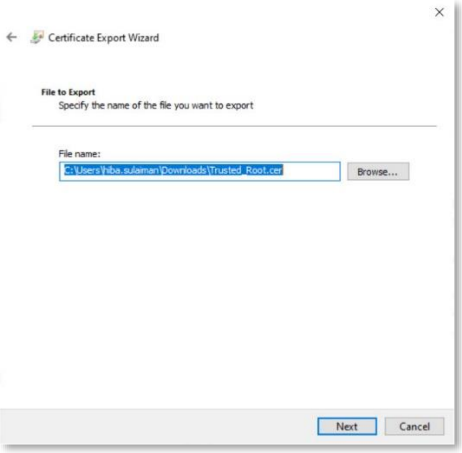


Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  □ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
  □ Include all certificates in the certification path if possible
  □ Delete the private key if the export is successful
  □ Export all extended properties
  □ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

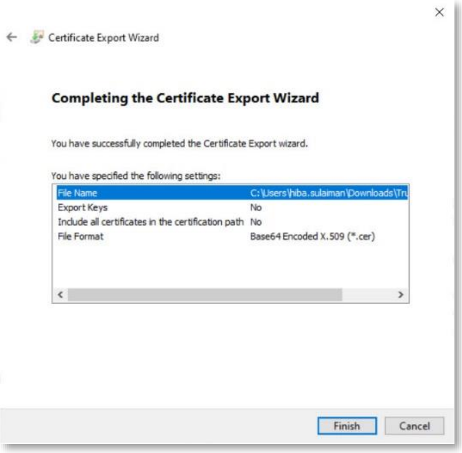
5. In the next step, specify the name of the file you want to export e.g. Trust_Cert and click Next.



File to Export
Specify the name of the file you want to export

File name: C:\Users\hiba.sulaiman\Downloads\Trusted_Root.cer

6. Click Finish to complete the Certificate Export Wizard.



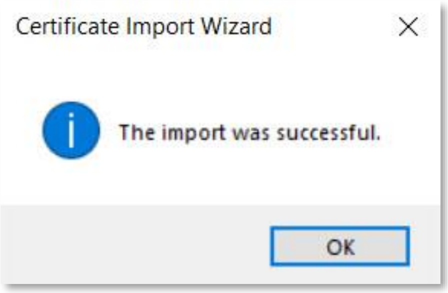
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\hiba.sulaiman\Downloads\Tru
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

7. Once your certificate is imported, the following screen will appear. Click OK.



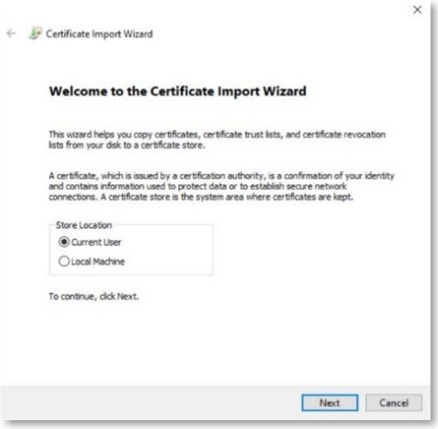
The import was successful.

You have successfully extracted the chain of certificates that will be required to get certificates trusted in the Microsoft Intune Admin Centre.

The next step is to download the certificates on your deployment machine:

1. The certificate will be exported to your Downloads folder.

Right-click on your certificate e.g. Trusted_Certificate.cer, and click Install certificate. The Certificate Import Wizard will appear. Select the Current User and click Next.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

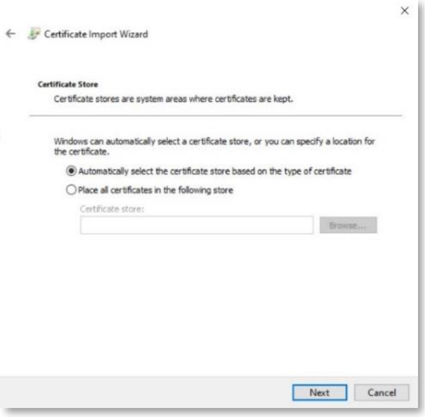
Store Location

● Current User

○ Local Machine

To continue, click Next.

2. The Certificate Store screen will appear, choose your destination folder, or select automatically select the certificate store based on the type of certificate, and click Next.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

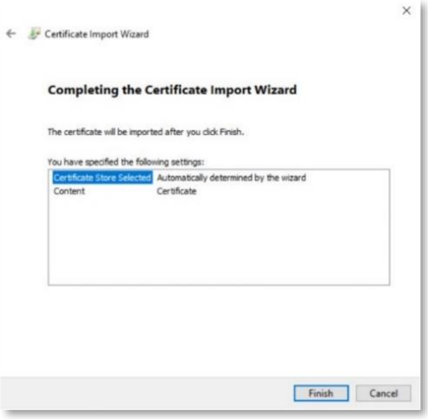
Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

3. To complete the Certificate Import Wizard, click Finish.



Certificate Import Wizard

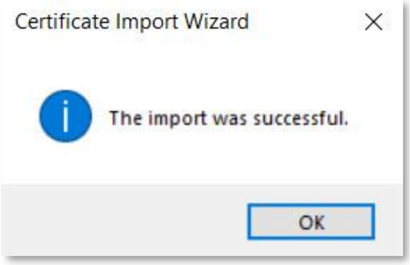
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

4. Once your certificate is imported, the following screen will appear. Click OK.



Certificate Import Wizard

The import was successful.

You have successfully downloaded the certificate on your machine.

3.2. ADSS Web RA Server Pre-Requisites

Before configuring ADSS Web RA Server for Microsoft Intune, you will need the following:

- Root CA Certificate from ADSS Server.
- Certificate Templates, ADSS Certificate Profiles, Client ID and Secret from ADSS Server.
- Microsoft Certificate Templates to map to ADSS Server Certificate Templates.
- Microsoft Azure Active Directory.

4 Installing ADSS Web RA Server

ADSS Web RA Server should be installed by following the installation steps defined within the product installation guide.

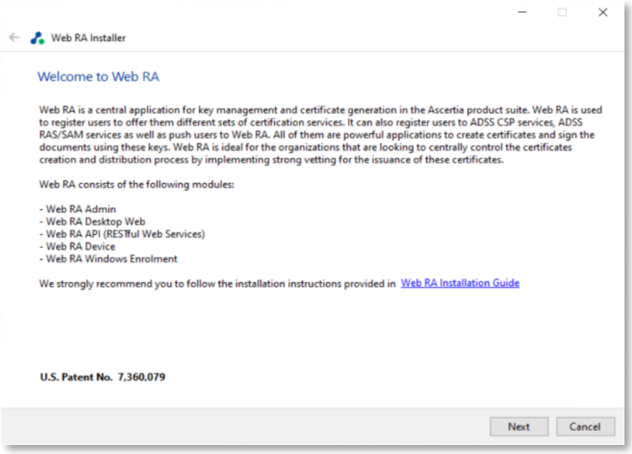
- IIS 10+ required features.
- ASP.NET Core Runtime 7.0.0 or above
- IIS URL Rewrite Module.

4.3. ADSS Web RA Installation

The Microsoft Intune SCEP feature will only be available when the administrator installs the latest ADSS Web RA Server package from the installer.

1. Extract the ADSS Web RA Server installation package to the following path:

   ```
   C:\ascertia\WebRA-v2.9-Win64-11Sep2023
   ```
2. Using Windows Explorer, navigate to C:\ascertia\WebRA-v2.9-Win64-11Sep2023\setup, double click install.bat
3. The Web RA installer will launch, at the Welcome dialog, click Next.



Welcome to Web RA

Web RA is a central application for key management and certificate generation in the Ascertia product suite. Web RA is used to register users to offer them different sets of certification services. It can also register users to ADSS CSP services, ADSS RAS/SAM services as well as push users to Web RA. All of them are powerful applications to create certificates and sign the documents using these keys. Web RA is ideal for the organizations that are looking to centrally control the certificates creation and distribution process by implementing strong vetting for the issuance of these certificates.

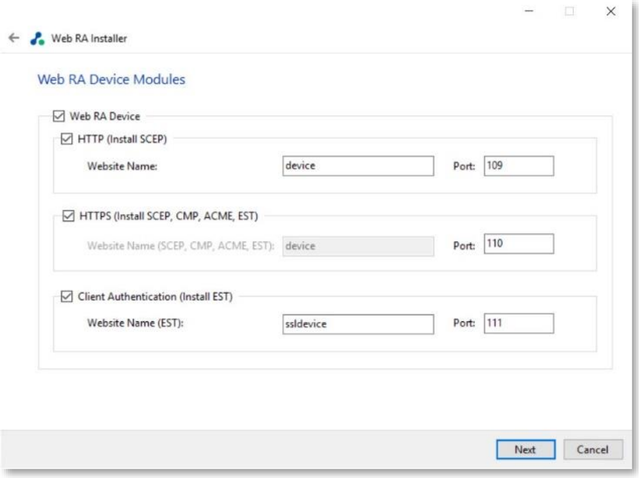
Web RA consists of the following modules:

- Web RA Admin
- Web RA Desktop Web
- Web RA API (RESTful Web Services)
- Web RA Device
- Web RA Windows Enrolment

We strongly recommend you to follow the installation instructions provided in Web RA Installation Guide

U.S. Patent No. 7,360,079

4. The Web RA Device Modules dialog will display, Select the Web RA Device checkbox. Click Next. For each selected application, provide the web application name and port. Click Next to proceed.



Web RA Device Modules

☑ Web RA Device

☑ HTTP (Install SCEP)

Website Name: device Port: 109

☑ HTTPS (Install SCEP, CMP, ACME, EST)

Website Name (SCEP, CMP, ACME, EST): device Port: 110

☑ Client Authentication (Install EST)

Website Name (EST): ssldevice Port: 111

Please refer to the ADSS Web RA installation guide for detailed steps for the installation process.

5 ADSS Web RA Server Integration with Microsoft Intune

Before configuring the Microsoft Intune SCEP feature, the following pre-requisites from the ADSS Web RA Server are necessary:

- External connectors for:
    - ADSS Server
    - SMTP Server
    - Microsoft Azure Active Directory
    - Certification Profiles created for ADSS Server and Web RA.

- Create a service plan.
- Create an enterprise.
- Import a license and allocate certificate quantities to the test enterprise.
- Create a default role with Microsoft Intune SCEP profile.
- Share certificate using the SDNs filter in the specific role.
- Set SCEP protocol in the enrolment protocol (s) section.

This part of the document describes the configurations in the ADSS Web RA Server as a third-party SCEP enrolment server for Microsoft Intune certificate enrolment.

Before you begin, you need to ensure that you have the following items:

1. Microsoft Authenticator on your mobile device.
2. Intune Company Portal app on your Android mobile device.
3. Intune Company Portal app on your iOS mobile device.

5.1. ADSS Web RA Admin Portal

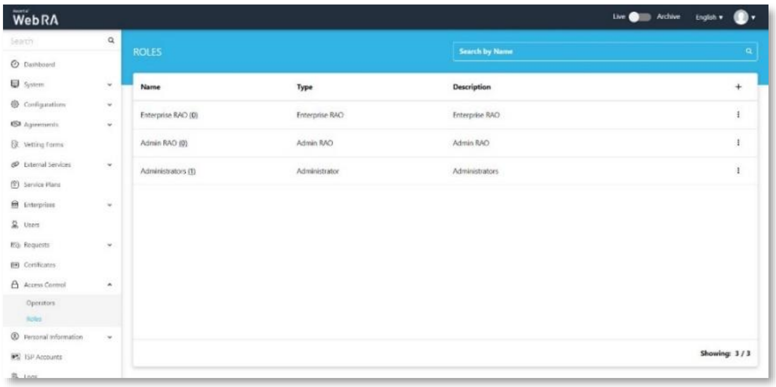
Following the installation of ADSS Web RA Server, the Intune SCEP feature must be enabled for any role who will need access to this feature. Use the following process to enable Microsoft Intune SCEP for the desired role.

5.1.1 Access Control

The default role i.e. Administrator, installed with ADSS Web RA Server has access to the Microsoft Intune SCEP feature. Apart from the administrator, other operators need to be enable it to configure the product.

4. Access ADSS Web RA administration portal as an administrator with permissions to assign the Microsoft Intune SCEP settings to roles.

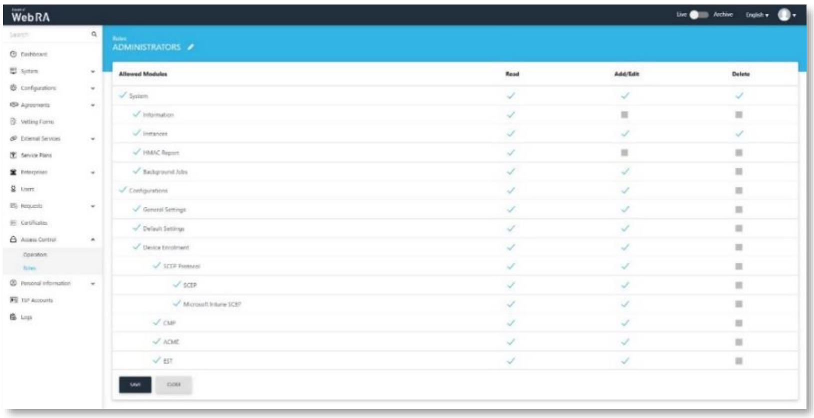
Navigate to Access Control > Roles > ⋮ > Edit.



Name	Type	Description	
Enterprise RAO (0)	Enterprise RAO	Enterprise RAO	⋮
Admin RAO (0)	Admin RAO	Admin RAO	⋮
Administrators (1)	Administrator	Administrators	⋮

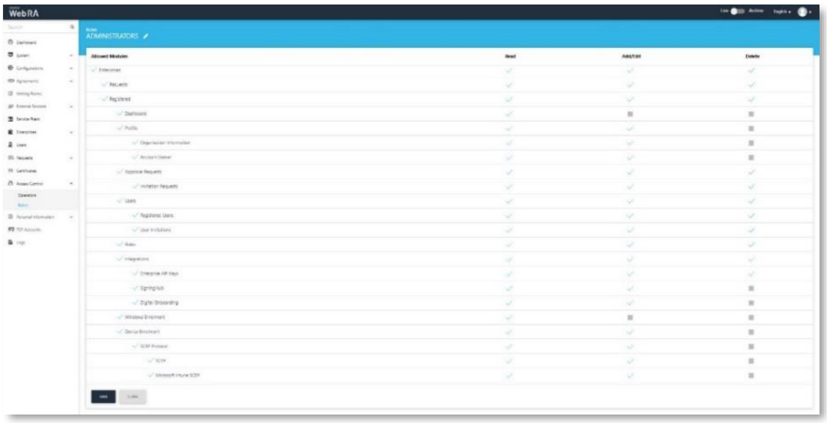
Showing: 3 / 3

5. Select Microsoft Intune SCEP check box from the Configurations, select Microsoft Intune SCEP under the Enterprise section and then click Save.



ADMINISTRATORS

Allowed Modules	Read	Add/Edit	Delete
✓ System	✓	✓	✓
✓ Information	✓	■	■
✓ Instances	✓	✓	✓
✓ HMAC Report	✓	■	■
✓ Background Jobs	✓	✓	■
✓ Configurations	✓	✓	■
✓ General Settings	✓	✓	■
✓ Default Settings	✓	✓	■
✓ Device Enrolment	✓	✓	■
✓ SCEP Protocol	✓	✓	■
✓ SCEP	✓	✓	■
✓ Microsoft Intune SCEP	✓	✓	■
✓ CMP	✓	✓	■
✓ ACME	✓	✓	■
✓ EST	✓	✓	■



ADMINISTRATORS

Allowed Modules	Read	Add/Edit	Delete
✓ Enterprises	✓	✓	✓
✓ Requests	✓	✓	✓
✓ Registered	✓	✓	✓
✓ Dashboard	✓	■	■
✓ Profile	✓	✓	■
✓ Organization Information	✓	✓	■
✓ Account Owner	✓	✓	■
✓ Approval Requests	✓	✓	✓
✓ Invitation Requests	✓	✓	✓
✓ Users	✓	✓	✓
✓ Registered Users	✓	✓	✓
✓ User Invitations	✓	✓	✓
✓ Roles	✓	✓	✓
✓ Integrations	✓	✓	✓
✓ Enterprise API Keys	✓	✓	✓
✓ SigningHub	✓	✓	■
✓ Digital Onboarding	✓	✓	■
✓ Windows Enrolment	✓	■	■
✓ Device Enrolment	✓	✓	■
✓ SCEP Protocol	✓	✓	■
✓ SCEP	✓	✓	■
✓ Microsoft Intune SCEP	✓	✓	■

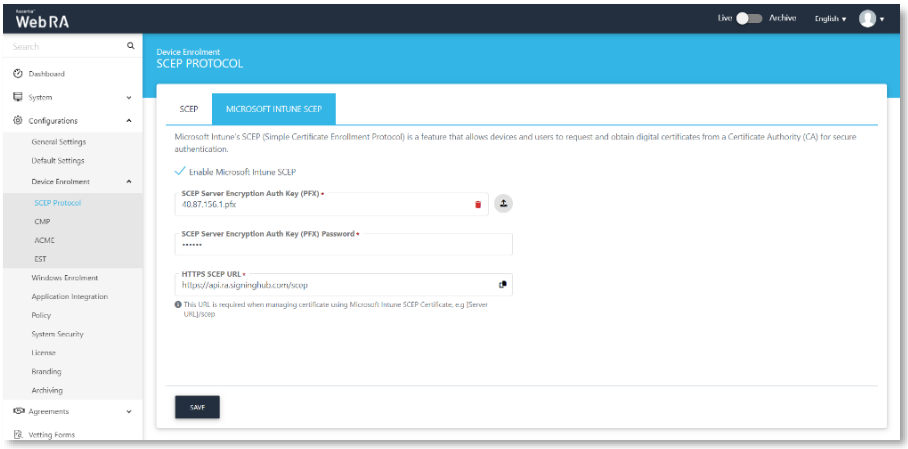
5.1.2 Configurations

You will be required to enable Intune SCEP in the configurations. Use the following process to enable SCEP for Microsoft Intune Certificate Enrolment.

Access Web RA administration portal as an administrator to enable Microsoft Intune SCEP feature.

1. Navigate to Configurations > Enrolment Protocol(s) > SCEP > Microsoft Intune SCEP.
2. Select the Enable Microsoft Intune SCEP checkbox.

- Upload a SCEP Server Encryption Auth Key (PFX)
- Enter the SCEP Server Encryption Auth Key (PFX) Password.
- Add the HTTPS SCEP URL that the devices will use to communicate with ADSS Web RA and click Save. (Make sure you upload PFX and chain of the same Root & Intermediate certificates that you will be using in ADSS Web RA and in Microsoft Intune).



Device Enrolment
SCEP PROTOCOL

SCEP | MICROSOFT INTUNE SCEP

Microsoft Intune's SCEP (Simple Certificate Enrollment Protocol) is a feature that allows devices and users to request and obtain digital certificates from a Certificate Authority (CA) for secure authentication.

✓ Enable Microsoft Intune SCEP

SCEP Server Encryption Auth Key (PFX) *: 40.87.156.1.pfx

SCEP Server Encryption Auth Key (PFX) Password *: ••••••

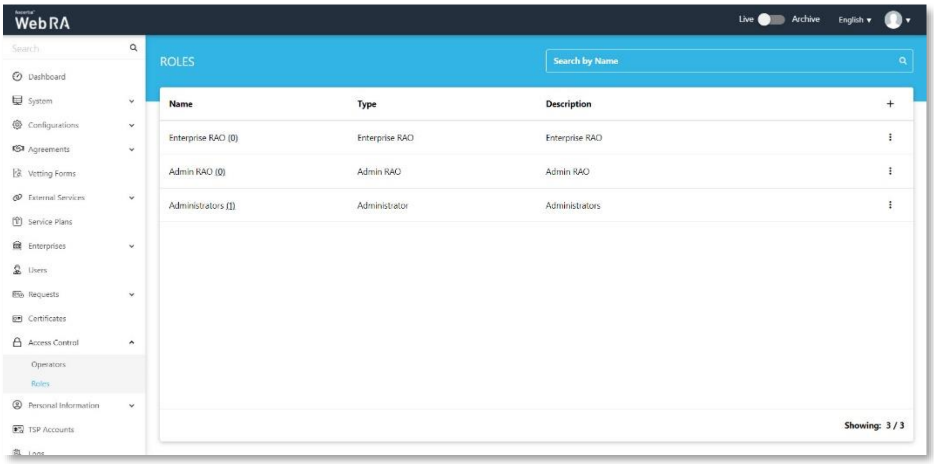
HTTPS SCEP URL *: https://api.ra.signinghub.com/scep

This URL is required when managing certificate using Microsoft Intune SCEP Certificate, e.g [Server URL]/scep

SAVE

5.1.3 Assign Modules to Administrators

1. Expand Access Control > Roles.
2. Click ⋮ against the administrator role.



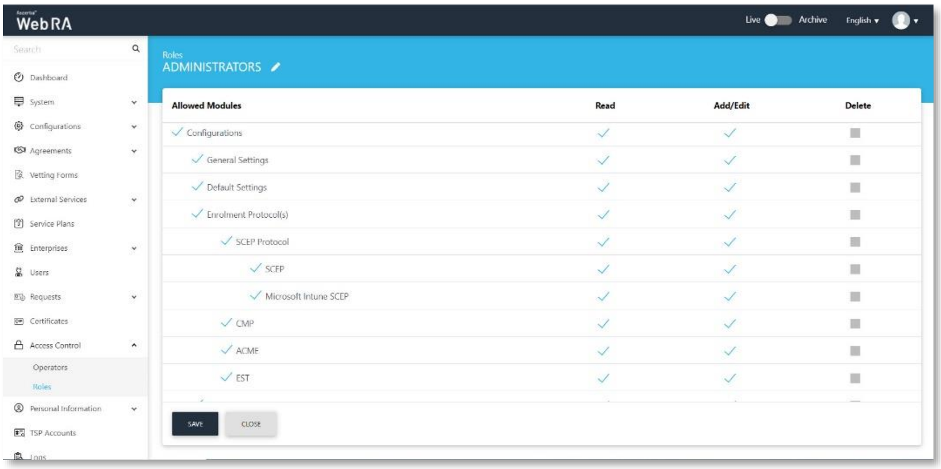
ROLES

Search by Name

Name	Type	Description	+
Enterprise RAO (0)	Enterprise RAO	Enterprise RAO	⋮
Admin RAO (0)	Admin RAO	Admin RAO	⋮
Administrators (1)	Administrator	Administrators	⋮

Showing: 3 / 3

3. In the Allowed Modules section, select the Enrolment Protocol (s) to enable SCEP and Microsoft Intune SCEP.



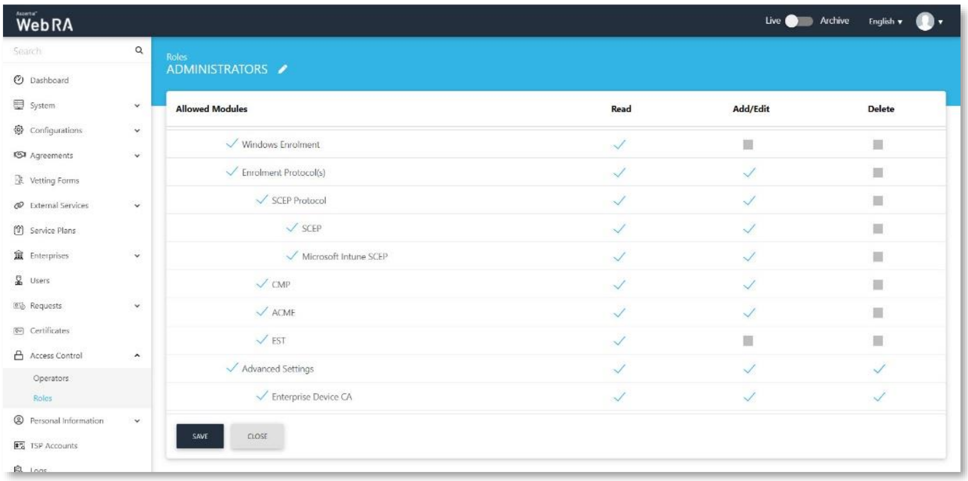
Roles
ADMINISTRATORS

Allowed Modules	Read	Add/Edit	Delete
✓ Configurations	✓	✓	■
✓ General Settings	✓	✓	■
✓ Default Settings	✓	✓	■
✓ Enrolment Protocol(s)	✓	✓	■
✓ SCEP Protocol	✓	✓	■
✓ SCEP	✓	✓	■
✓ Microsoft Intune SCEP	✓	✓	■
✓ CMP	✓	✓	■
✓ ACME	✓	✓	■
✓ EST	✓	✓	■

SAVE CLOSE

4. Scroll down, and from the Enterprise Role section

Select Enrolment Protocol (s) to enable and select SCEP Protocol, SCEP and Microsoft Intune SCEP. Then click Save.



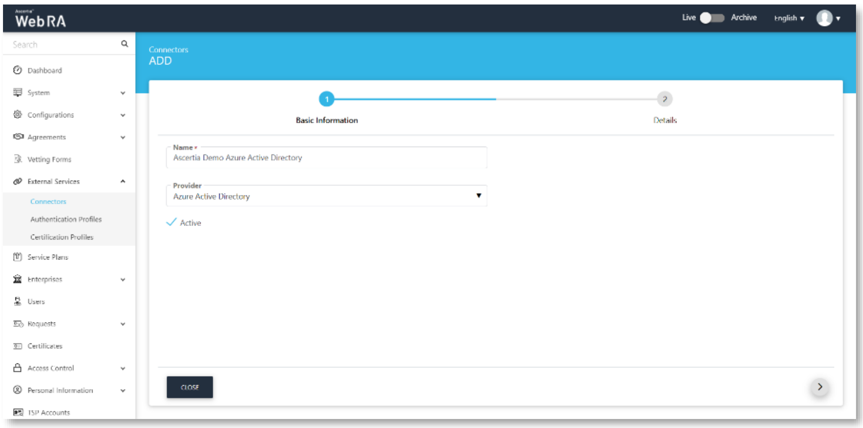
Roles
ADMINISTRATORS

Allowed Modules	Read	Add/Edit	Delete
✓ Windows Enrolment	✓	□	□
✓ Enrolment Protocol(s)	✓	✓	□
✓ SCEP Protocol	✓	✓	□
✓ SCEP	✓	✓	□
✓ Microsoft Intune SCEP	✓	✓	□
✓ CMP	✓	✓	□
✓ ACME	✓	✓	□
✓ EST	✓	□	□
✓ Advanced Settings	✓	✓	✓
✓ Enterprise Device CA	✓	✓	✓

5.1.4 Create Azure Active Directory Connector

In order to create a certificate, ADSS Web RA Server requires an Azure Active Directory connector. This section provides the configuration steps to create this connector.

1. Expand External Services > Connectors > click +
2. The basic information page will display, Enter a name and select Azure Active Directory from the provider drop-down, tick the Active check box, click >.



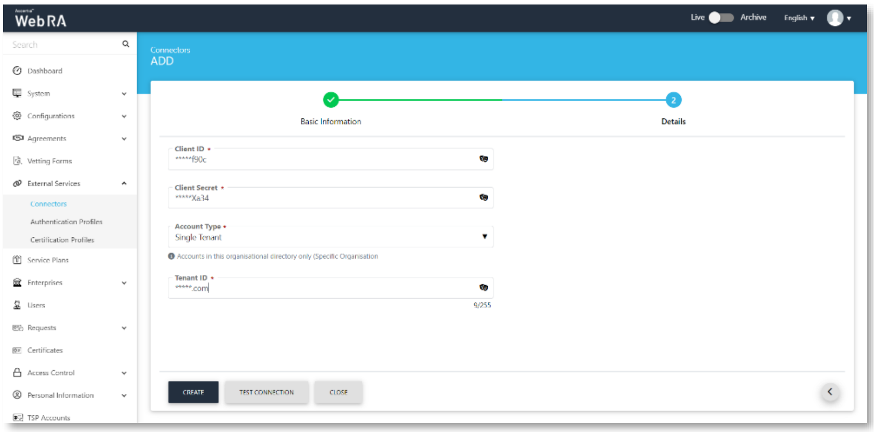
Connectors
ADD

Name *
Ascertia Demo Azure Active Directory

Provider
Azure Active Directory

✓ Active

3. The Details page will display, enter the Client ID, Client Secret, Account Type and Tenant ID. Then click Create.



Connectors
ADD

Client ID *
*****f90c

Client Secret *
*****Xa34

Account Type *
Single Tenant

Accounts in this organisational directory only (Specific Organisation

Tenant ID *
*****.com

9/255

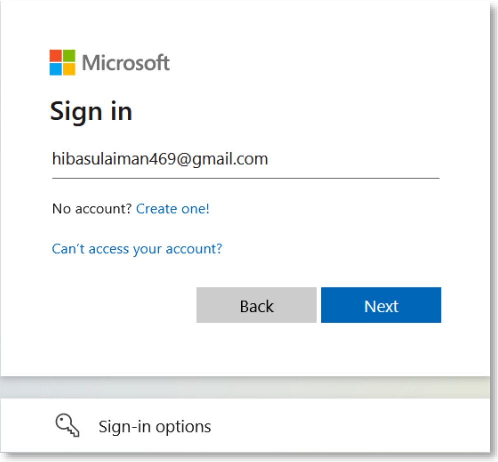
You are required to register an application in the Azure AD portal to get the client ID, client secret and tenant ID.

In order to enable a third-party SCEP server to perform customized challenge validation through Microsoft Intune, create an application in Azure AD. This application grants Intune the necessary privileges to authenticate SCEP requests.

5.1.5 Sign up for Microsoft Intune

1. To sign up Microsoft Intune, click Dashboard - Microsoft 365 Dev Center

Enter an active email address (preferably a Gmail account), and then click Next.



Microsoft

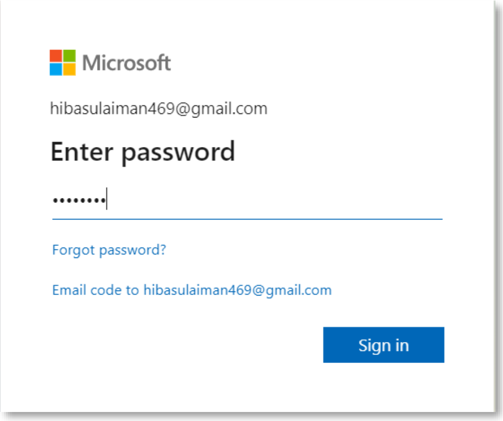
Sign in

hibasulaiman469@gmail.com

No account? Create one!

Can't access your account?

2. Enter password, and then click Sign in.



Microsoft

hibasulaiman469@gmail.com

Enter password

••••••••

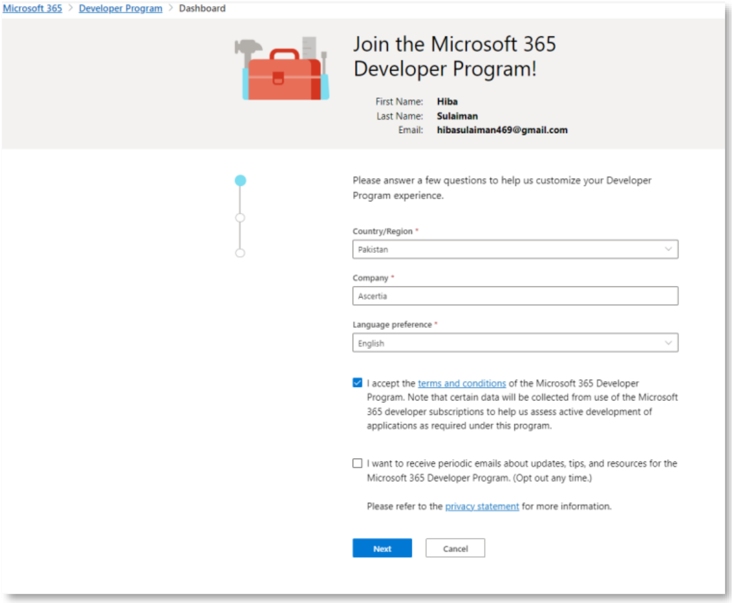
Forgot password?

Email code to hibasulaiman469@gmail.com

3. Enter the following:

- Country Name
- Company
- Language preferences
- Select I accept the terms and conditions…

Click Next.



Microsoft 365 > Developer Program > Dashboard

Join the Microsoft 365 Developer Program!

First Name: **Hiba**
Last Name: **Sulaiman**
Email: **hibasulaiman469@gmail.com**

Please answer a few questions to help us customize your Developer Program experience.

Country/Region *
Pakistan

Company *
Ascertia

Language preference *
English

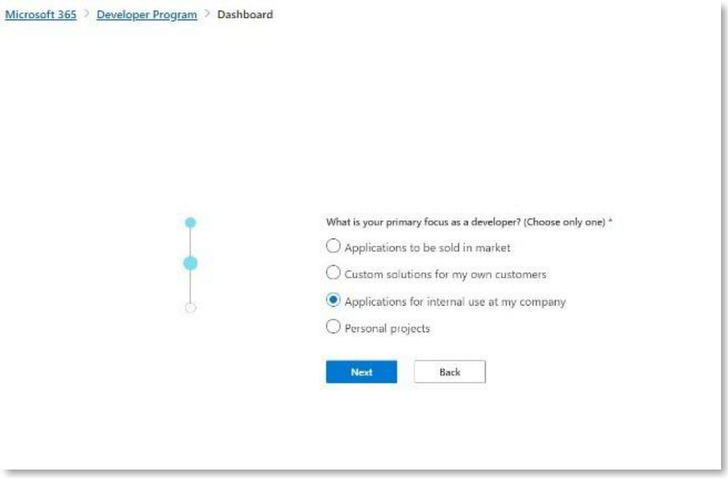
☑ I accept the terms and conditions of the Microsoft 365 Developer Program. Note that certain data will be collected from use of the Microsoft 365 developer subscriptions to help us assess active development of applications as required under this program.

☐ I want to receive periodic emails about updates, tips, and resources for the Microsoft 365 Developer Program. (Opt out any time.)

Please refer to the privacy statement for more information.

4. Choose an option depending on your requirement.

In this scenario, we have selected Applications for internal use at my company. Then click Next.

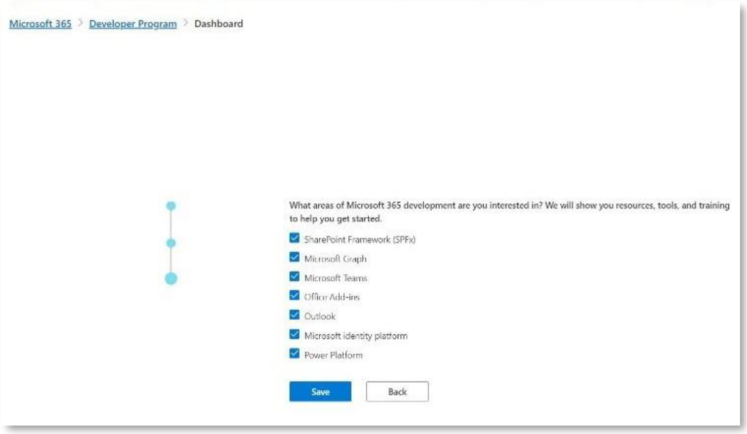


Microsoft 365 > Developer Program > Dashboard

What is your primary focus as a developer? (Choose only one) *

○ Applications to be sold in market
○ Custom solutions for my own customers
● Applications for internal use at my company
○ Personal projects

5. On the next screen, make sure you select all the tools and resources as displayed below. Selecting all options is necessary as all Microsoft tools are interconnected and are required for Microsoft Intune, and click Save.

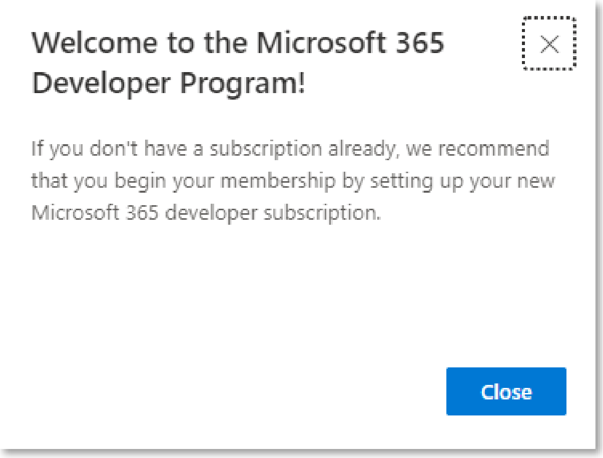


Microsoft 365 > Developer Program > Dashboard

What areas of Microsoft 365 development are you interested in? We will show you resources, tools, and training to help you get started.

☑ SharePoint Framework (SPFx)
☑ Microsoft Graph
☑ Microsoft Teams
☑ Office Add-ins
☑ Outlook
☑ Microsoft identity platform
☑ Power Platform

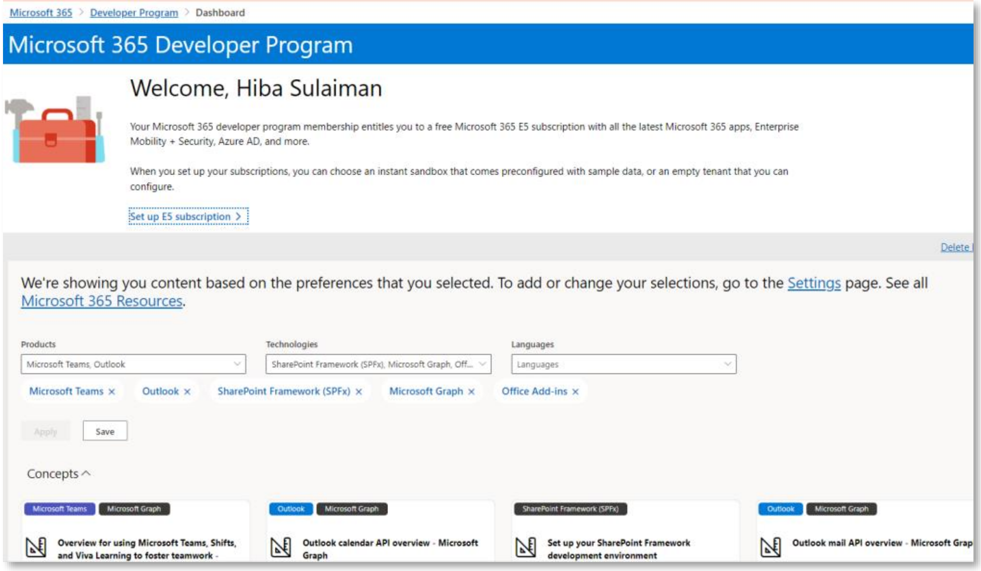
6. The Welcome screen will appear, click Close.



Welcome to the Microsoft 365 Developer Program!

If you don't have a subscription already, we recommend that you begin your membership by setting up your new Microsoft 365 developer subscription.

7. From the Welcome screen, click Set up E5 subscription.



Microsoft 365 > Developer Program > Dashboard

Microsoft 365 Developer Program

Welcome, Hiba Sulaiman

Your Microsoft 365 developer program membership entitles you to a free Microsoft 365 E5 subscription with all the latest Microsoft 365 apps, Enterprise Mobility + Security, Azure AD, and more.

When you set up your subscriptions, you can choose an instant sandbox that comes preconfigured with sample data, or an empty tenant that you can configure.

Set up E5 subscription >

We're showing you content based on the preferences that you selected. To add or change your selections, go to the Settings page. See all Microsoft 365 Resources.

Products: Microsoft Teams, Outlook

Technologies: SharePoint Framework (SPFx), Microsoft Graph, Off...

Languages: Languages

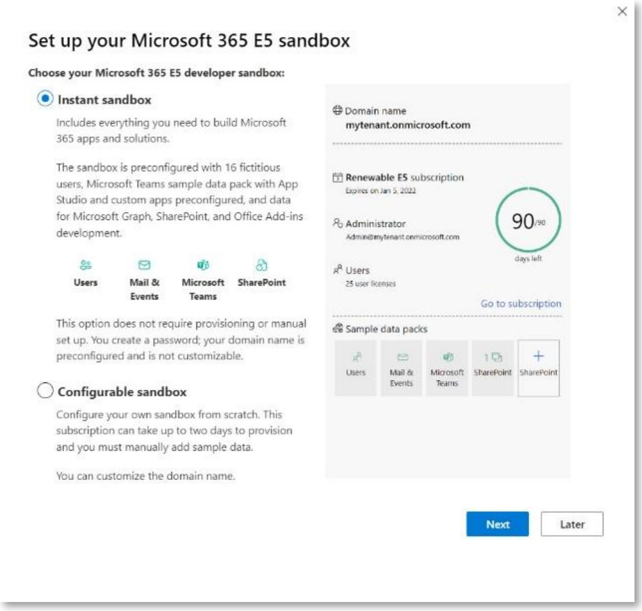
Overview for using Microsoft Teams, Shifts, and Viva Learning to foster teamwork -

Outlook calendar API overview - Microsoft Graph

Set up your SharePoint Framework development environment

Outlook mail API overview - Microsoft Grap

8. Select the Instant sandbox option and click Next to proceed.



Set up your Microsoft 365 E5 sandbox

Choose your Microsoft 365 E5 developer sandbox:

● Instant sandbox

Includes everything you need to build Microsoft 365 apps and solutions.

The sandbox is preconfigured with 16 fictitious users, Microsoft Teams sample data pack with App Studio and custom apps preconfigured, and data for Microsoft Graph, SharePoint, and Office Add-ins development.

This option does not require provisioning or manual set up. You create a password; your domain name is preconfigured and is not customizable.

○ Configurable sandbox

Configure your own sandbox from scratch. This subscription can take up to two days to provision and you must manually add sample data.

You can customize the domain name.

Domain name: mytenant.onmicrosoft.com

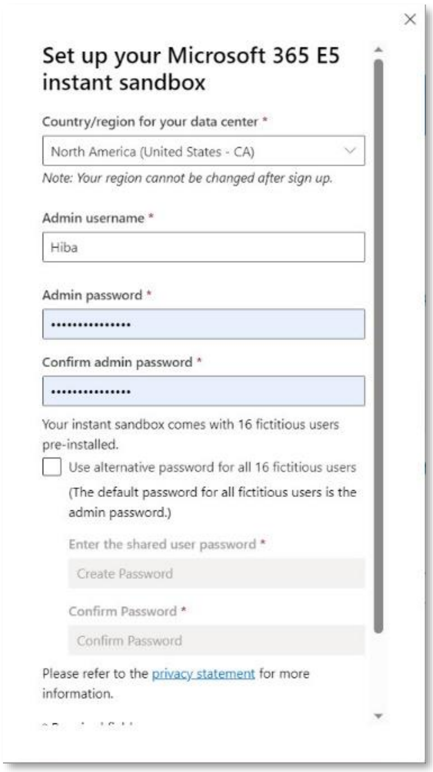
Renewable E5 subscription: Expires on Jan 5, 2022

Administrator: Admin@mytenant.onmicrosoft.com

Users: 25 user licenses

9. Select and fill the following:

- Country
- Set up your user name
- Set up your password, and then click Next.



Set up your Microsoft 365 E5 instant sandbox

Country/region for your data center *

North America (United States - CA)

Note: Your region cannot be changed after sign up.

Admin username *

Hiba

Admin password *

•••••••••••••••

Confirm admin password *

•••••••••••••••

Your instant sandbox comes with 16 fictitious users pre-installed.

□ Use alternative password for all 16 fictitious users

(The default password for all fictitious users is the admin password.)

Enter the shared user password *

Create Password

Confirm Password *

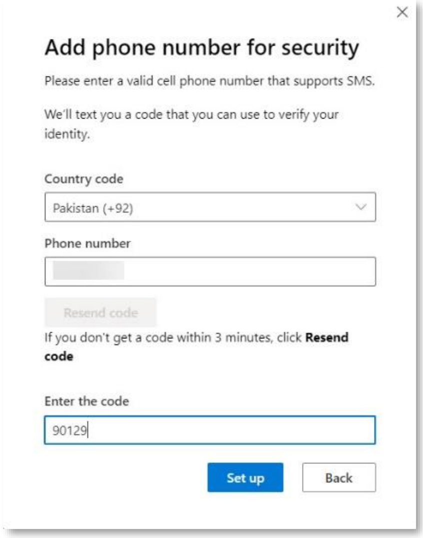
Confirm Password

Please refer to the privacy statement for more information.

10. Add the following:

- Country Code
- Phone Number
- Click Send Code.

Once you receive the code on your mobile number, enter it and click Set up.



Add phone number for security

Please enter a valid cell phone number that supports SMS.

We'll text you a code that you can use to verify your identity.

Country code

Pakistan (+92)

Phone number

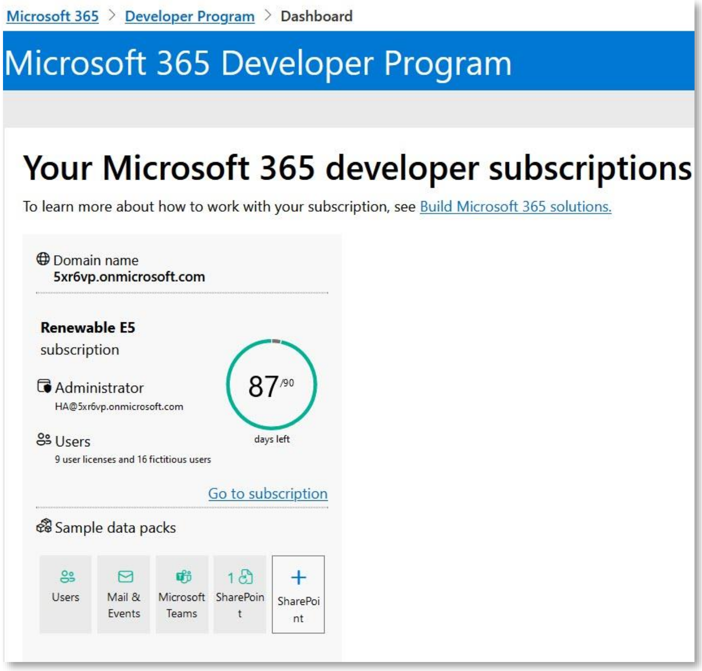
[redacted]

If you don't get a code within 3 minutes, click **Resend code**

Enter the code

90129

11. You will be redirected to the Microsoft 365 developer subscriptions page with your domain name e.g. 5xr6vp.onmicrosoft.com and the administrator e.g. HA@5xr6vp.onmicrosoft.com.



Microsoft 365 > Developer Program > Dashboard

Microsoft 365 Developer Program

Your Microsoft 365 developer subscriptions

To learn more about how to work with your subscription, see Build Microsoft 365 solutions.

Domain name
5xr6vp.onmicrosoft.com

Renewable E5 subscription

Administrator
HA@5xr6vp.onmicrosoft.com

Users
9 user licenses and 16 fictitious users

87/90 days left

Go to subscription

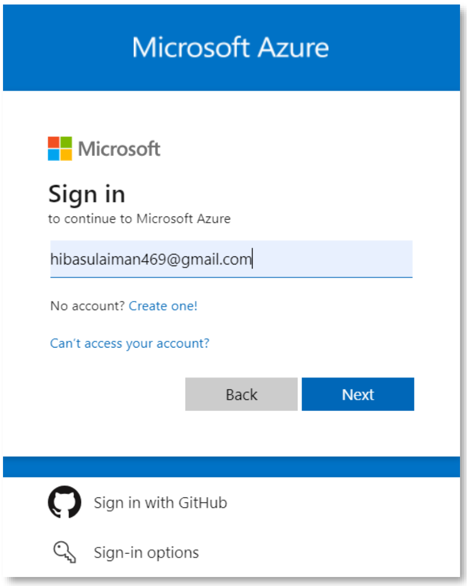
Sample data packs

12. If this page does not appear, refresh the Dashboard page, it will appear.

You have successfully completed the registration process for Microsoft Intune.

5.1.6 Create an application in Microsoft Azure Active Directory

1. Log in to the Azure Portal by following this link https://portal.azure.com/. You will be required to sign in with a Microsoft account to login. Use the same email address you used to sign up for Microsoft Intune in step 5.1.5. Enter email address, and then click Next.



Microsoft Azure

Microsoft

Sign in

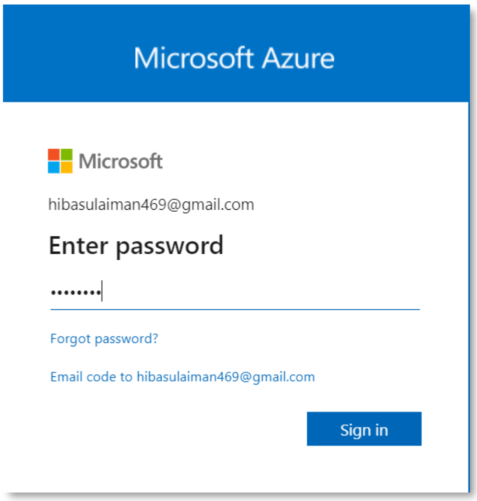
to continue to Microsoft Azure

hibasulaiman469@gmail.com

No account? Create one!

Can't access your account?

2. Enter the password, and click Sign in.



Microsoft Azure

Microsoft

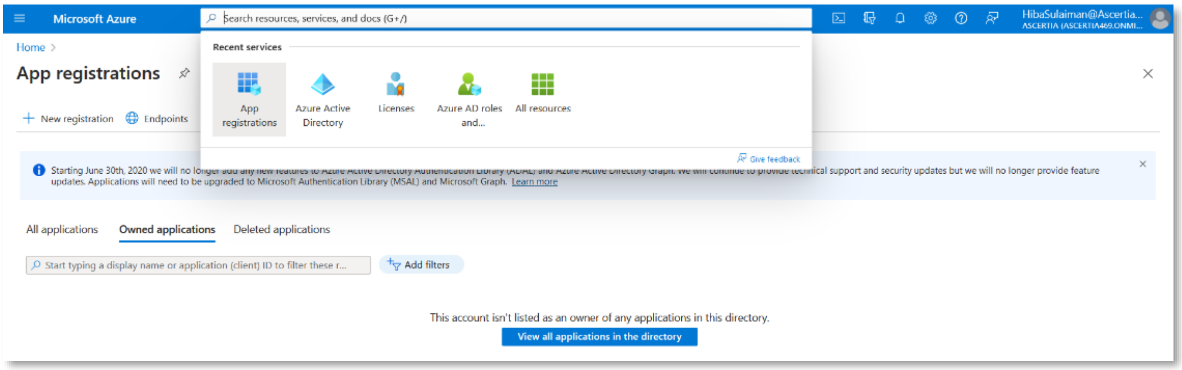
hibasulaiman469@gmail.com

Enter password

••••••••

You will be directed to the Home page.

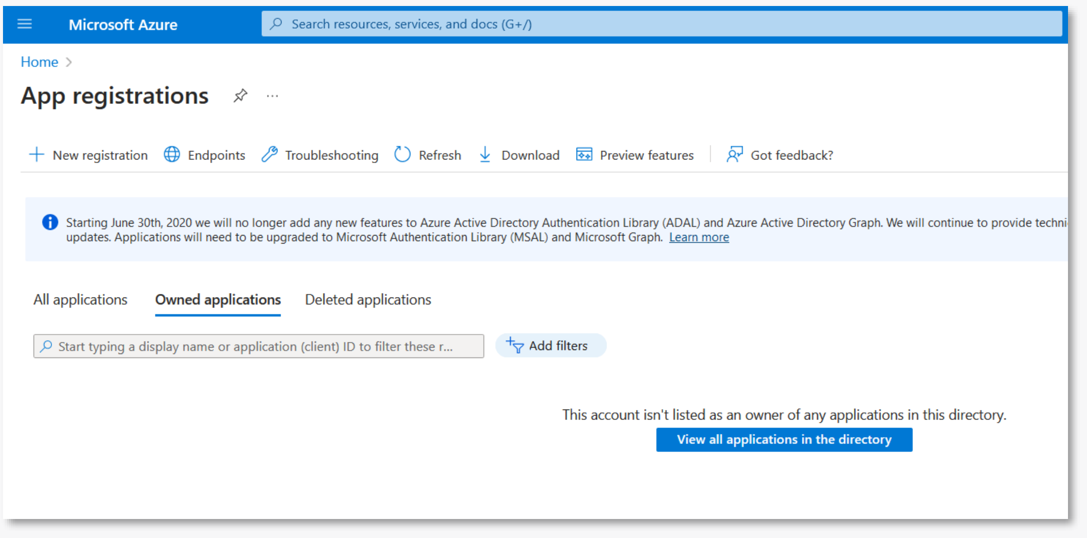
3. Search and click App Registrations in the Search Bar.



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

This account isn't listed as an owner of any applications in this directory.

4. Click New registration.

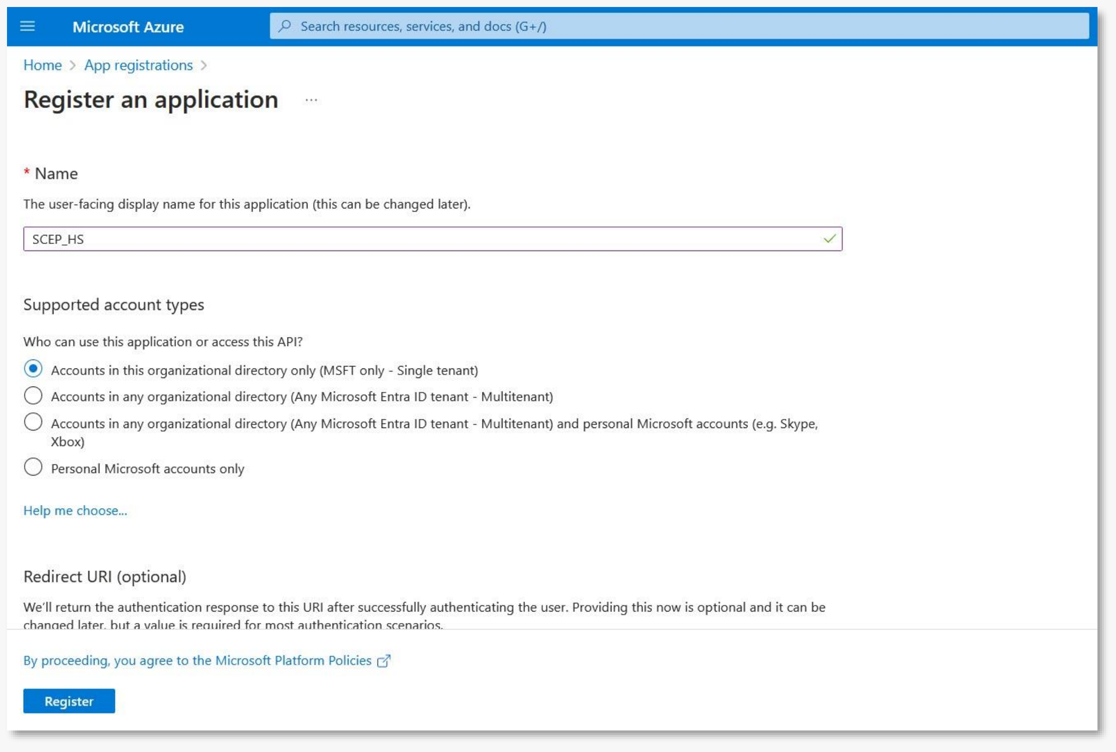


Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide techni updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

This account isn't listed as an owner of any applications in this directory.

5. On the Register an Application, fill in the required fields:

- Set a Name of the application, e.g. SCEP_HS.
- In Supported account types, select Accounts in this organizational directory only.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SCEP_HS

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (MSFT only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

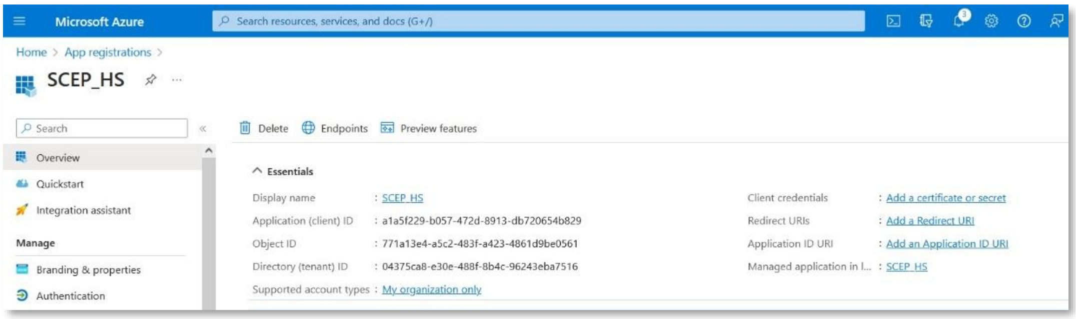
Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

By proceeding, you agree to the Microsoft Platform Policies

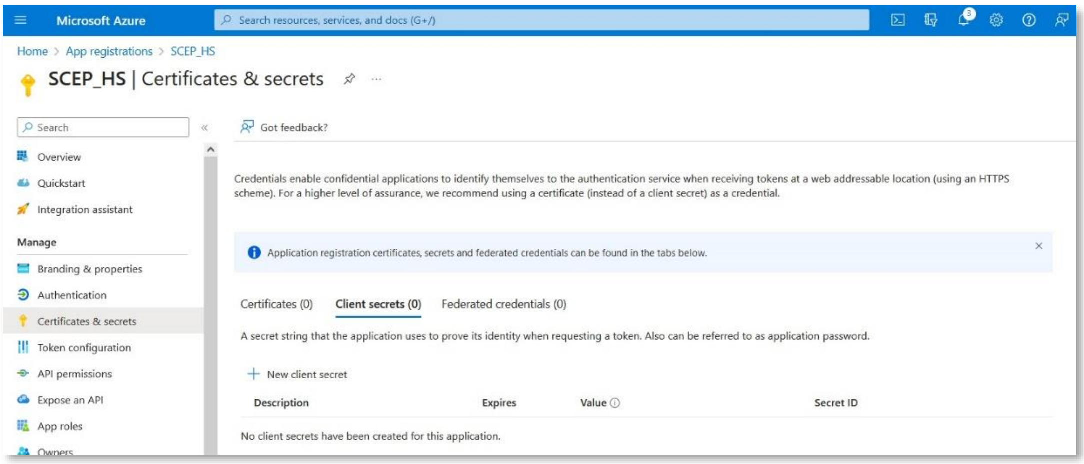
6. Click Register to create the application.



Display name : SCEP_HS
Application (client) ID : a1a5f229-b057-472d-8913-db720654b829
Object ID : 771a13e4-a5c2-483f-a423-4861d9be0561
Directory (tenant) ID : 04375ca8-e30e-488f-8b4c-96243eba7516
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : SCEP_HS

The details of the registered app will appear. Save the Application (client) ID as you will need it later while creating a connector in ADSS Web RA.

7. Click Add a certificate or secret on right side against client credentials. The following screen will appear. Click New client secret.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

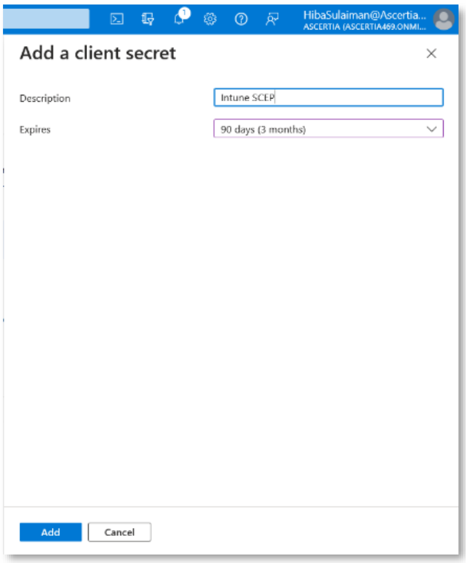
Description	Expires	Value	Secret ID

No client secrets have been created for this application.

8. Specify the following:

- Description, e.g. Intune SCEP
- Select an expiry, e.g. 90 days (3 months)

Then click Add to generate a value for the client secret.



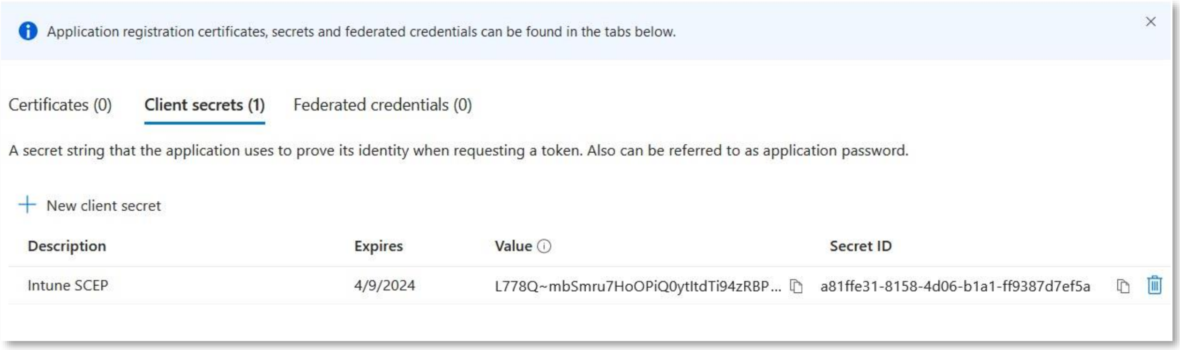
HibaSulaiman@Ascertia...
ASCERTIA (ASCERTIA469.ONMI...

Add a client secret

Description: Intune SCEP

Expires: 90 days (3 months)

9. Save the new client secret value as it is known as the Client Secret, required in the ADSS Web RA's connector.

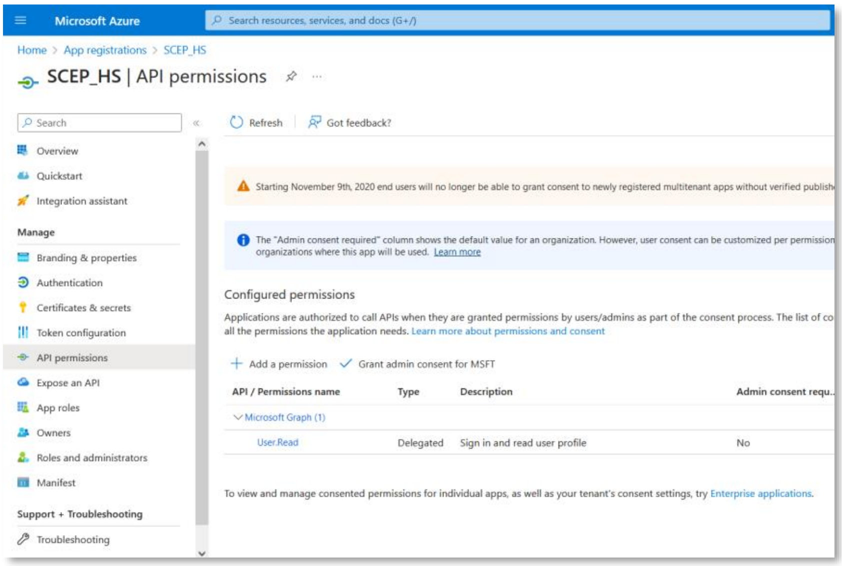


Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Intune SCEP	4/9/2024	L778Q~mbSmru7HoOPiQ0ytItdTi94zRBP...	a81ffe31-8158-4d06-b1a1-ff9387d7ef5a

10. From the left pane under Manage, select API permissions



Microsoft Azure
Search resources, services, and docs (G+/)
Home > App registrations > SCEP_HS

SCEP_HS | API permissions

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publish

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and consent

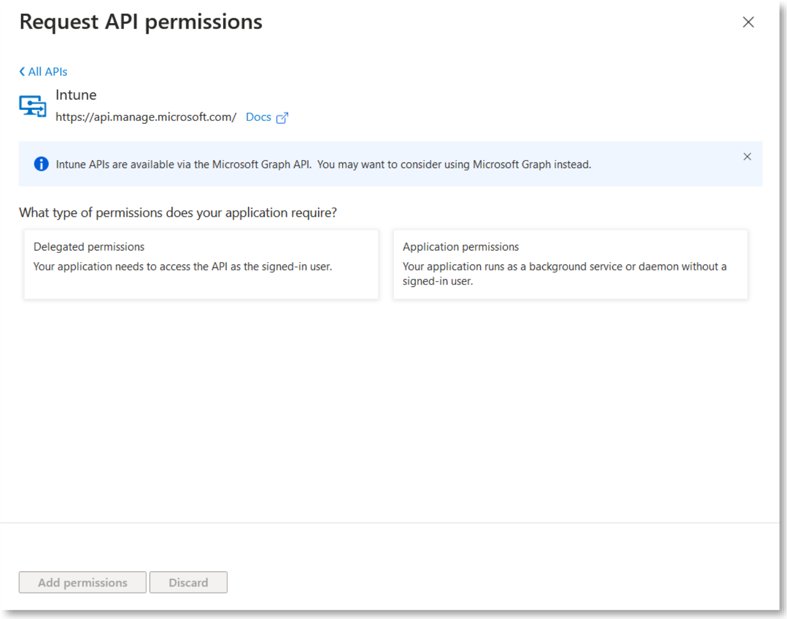
API / Permissions name	Type	Description	Admin consent requ...
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Then perform the following steps to add two separate API permissions:

1. Click Add a permission.

- On the Request API permissions page, select Intune, and then click Application permissions.



Request API permissions

< All APIs

Intune
https://api.manage.microsoft.com/ Docs

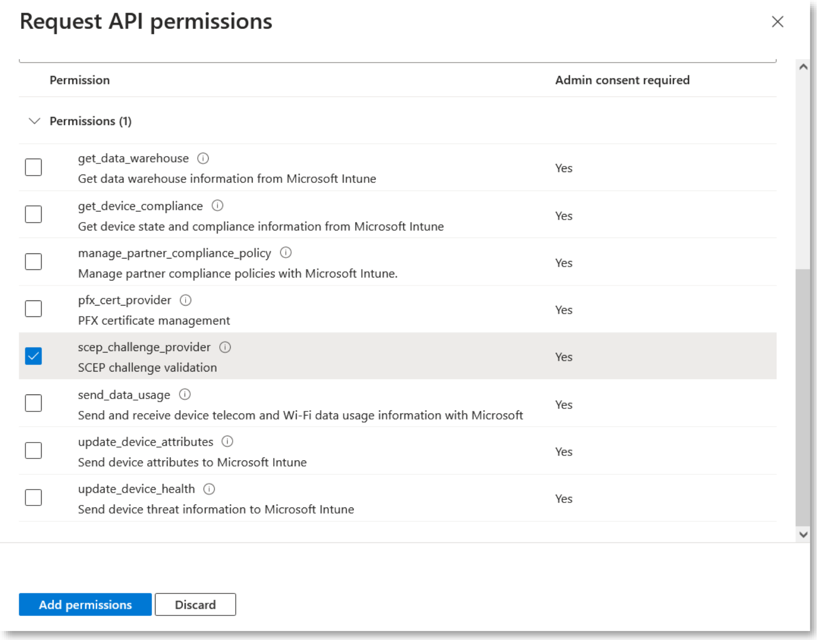
Intune APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

- Select the permission scep_challenge_provider (SCEP challenge validation), and then click Add permissions to save the configuration.



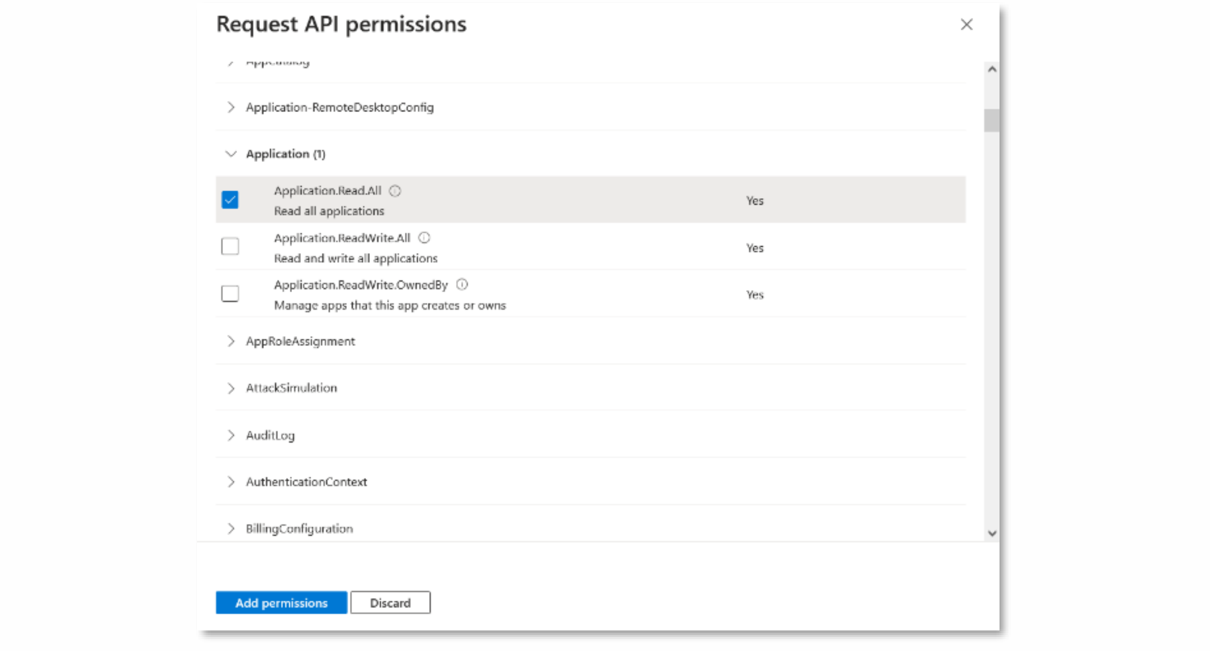
Request API permissions

Permissions (1)

	Permission	Admin consent required
□	get_data_warehouse Get data warehouse information from Microsoft Intune	Yes
□	get_device_compliance Get device state and compliance information from Microsoft Intune	Yes
□	manage_partner_compliance_policy Manage partner compliance policies with Microsoft Intune.	Yes
□	pfx_cert_provider PFX certificate management	Yes
☑	scep_challenge_provider SCEP challenge validation	Yes
□	send_data_usage Send and receive device telecom and Wi-Fi data usage information with Microsoft	Yes
□	update_device_attributes Send device attributes to Microsoft Intune	Yes
□	update_device_health Send device threat information to Microsoft Intune	Yes

2. Click Add a permission, again.

- On the Request API permissions page, select Microsoft Graph > Application permissions.
- Expand Application and select Application.Read.All (Read all applications), and click Add permissions to save the configuration.



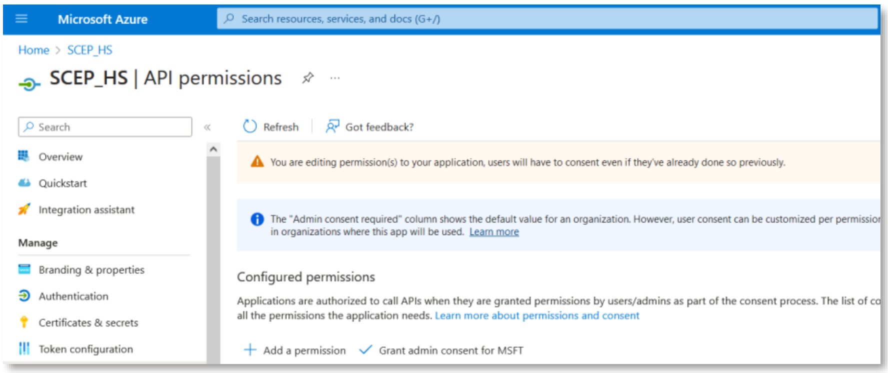
Request API permissions

- Application-RemoteDesktopConfig
- Application (1)

☑	Application.Read.All Read all applications	Yes
☐	Application.ReadWrite.All Read and write all applications	Yes
☐	Application.ReadWrite.OwnedBy Manage apps that this app creates or owns	Yes

- AppRoleAssignment
- AttackSimulation
- AuditLog
- AuthenticationContext
- BillingConfiguration

3. On the API permissions page under the Configured permissions, click Grant admin consent for <Tenant name>, e.g: Grant admin consent for MSFT.



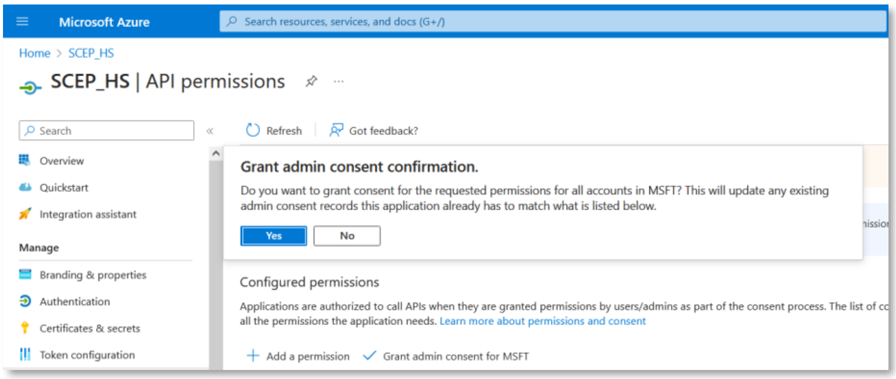
You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permissio in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and consent

4. Then click Yes when the grant consent confirmation appears.



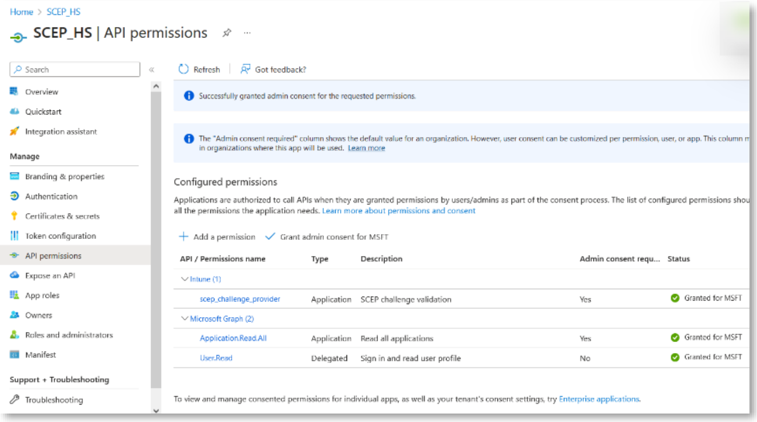
Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in MSFT? This will update any existing admin consent records this application already has to match what is listed below.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and consent

The success message will appear.



Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column m in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions shou all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Intune (1)				
scep_challenge_provider	Application	SCEP challenge validation	Yes	Granted for MSFT
Microsoft Graph (2)				
Application.Read.All	Application	Read all applications	Yes	Granted for MSFT
User.Read	Delegated	Sign in and read user profile	No	Granted for MSFT

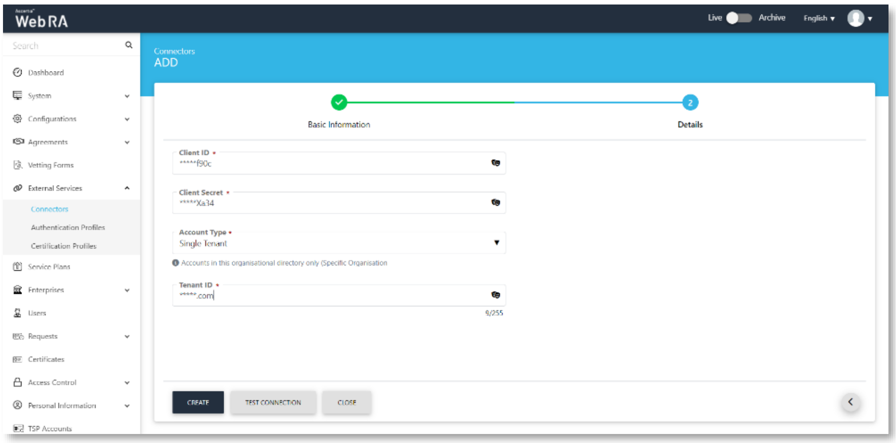
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

We can configure Microsoft Intune for the following platforms:

- Windows 10
- Android
- iOS

Azure AD connector

Now return to ADSS Web RA admin portal to complete the process of creating an Azure AD connector. Once you have created an application in the Azure AD in step 5.1.4 point 3, enter the client ID, client secret and tenant ID (from the app created in the Azure Portal) in the connector as displayed below and click Create.



Client ID *
*****f90c

Client Secret *
*****Xa34

Account Type *
Single Tenant ▾

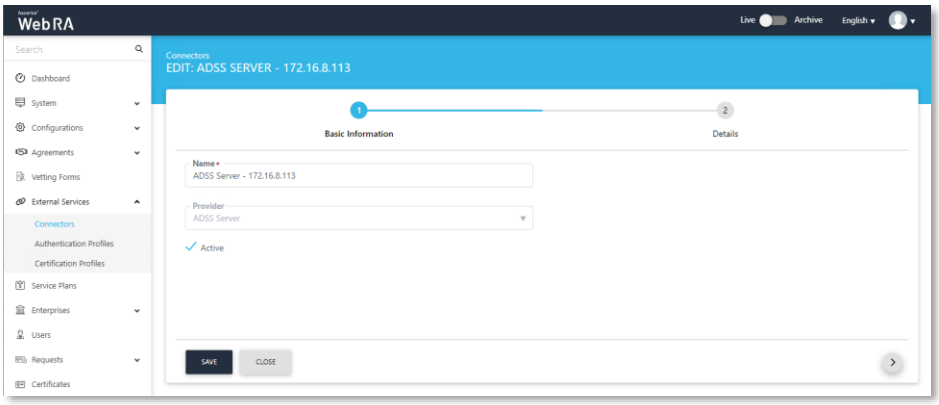
Accounts in this organisational directory only (Specific Organisation

Tenant ID *
*****.com
9/255

5.1.7 Create ADSS Server Connector

ADSS Web RA Server issues certificates from ADSS Server based Certification Authorities. This section provides steps to create the connector between Web RA Server and the ADSS Server Certification Service.

1. Expand External Services > Connectors > click +.
2. The Basic information page will display, enter a name and select ADSS Server as the provider, select the Active check box, click >.


Connectors
EDIT: ADSS SERVER - 172.16.8.113

Name *: ADSS Server - 172.16.8.113

Provider: ADSS Server

✓ Active

3. The Details page will display, provide the following information, click Create.

- Server Address

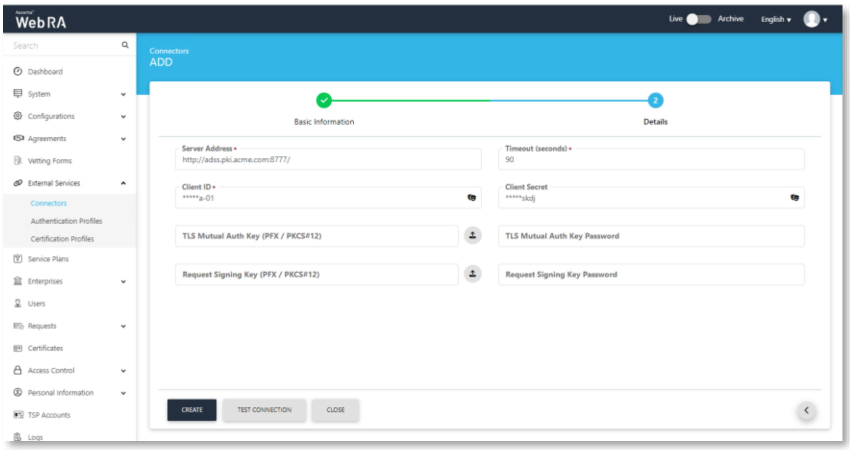
Specify the address and port number of ADSS Server.

- ADSS Client ID

Specify the ADSS Client ID configured in the Client Manager module of the ADSS Server for this connector.

- ADSS Client Secret

Specify the ADSS client secret generated in the ADSS Server against this Client ID.


Connectors
ADD

Server Address *: http://adss.pki.acme.com:8777/

Timeout (seconds) *: 90

Client ID *: *****a-01

Client Secret: *****skdj

TLS Mutual Auth Key (PFX / PKCS#12)

TLS Mutual Auth Key Password

Request Signing Key (PFX / PKCS#12)

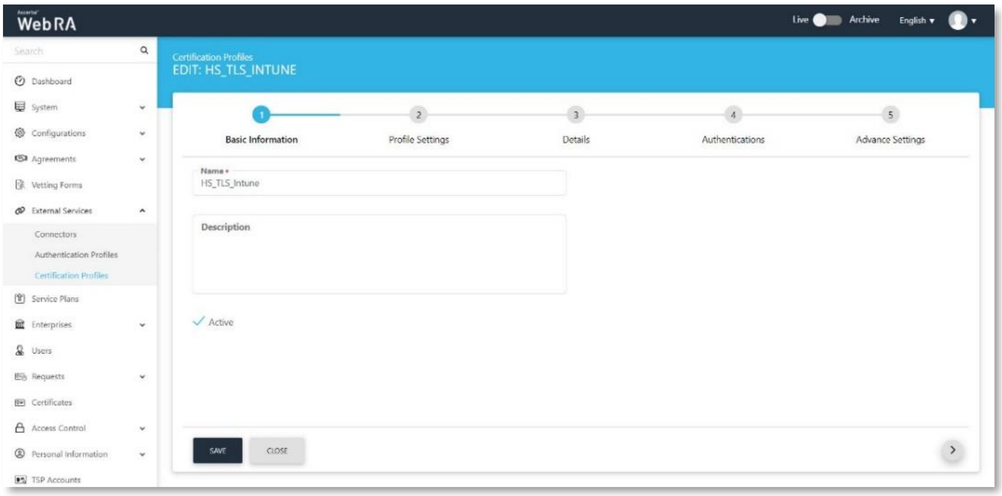
Request Signing Key Password

5.1.8 Create a Certification Profile

Azure Active Directory and ADSS Server maintain certificate templates that are used to generate keys and certificates for people, devices and applications. ADSS Web RA Server requires a certification profile for each type of certificate. It will be issuing using the Microsoft Intune SCEP feature, the following section provides steps on how to create a certification profile that maps a Microsoft Intune SCEP Certificate Template to an ADSS Server Certification profile and template to ensure that certificates are issued with the correct attributes, extensions, and validity periods.

The following is an example of creating a profile to support TLS User Authentication.

1. Expand External Services > Certification Profiles > click +.
2. The Basic information page will display, enter name, select the Active check box, click >.



Certification Profiles
EDIT: HS_TLS_INTUNE

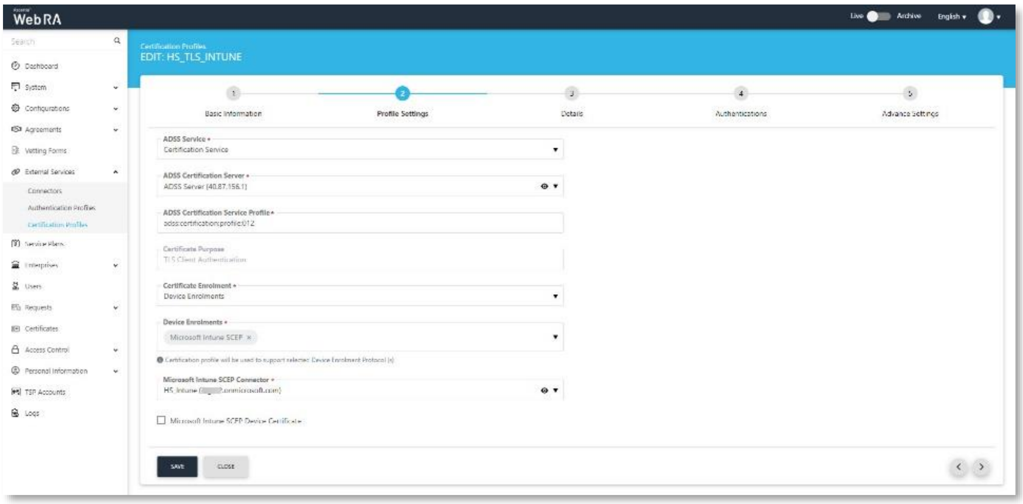
Name * HS_TLS_Intune

Description

✓ Active

3. The Profile Settings page will display, set the following, click >:

ADSS Service	Certification Service
ADSS Certification Server	Set the ADSS Server connector configured in step 5.1.6.
ADSS Certification Service Profile	Set the ADSS Server Certification Service Profile Name e.g. Windows TLS User - 1 Year
Certificate Purpose	This is auto set by ADSS Server
Certificate Enrolment	Select Enrolment Protocol(s)
Enrolment Protocol(s)	Select the SCEP, and Microsoft Intune SCEP protocols
Microsoft Intune SCEP connector	Set to the Azure Active Directory Connector created in step 5.1.4.
Microsoft Intune SCEP Device Certificate	Select this checkbox if you want to create a device certificate



Certification Profiles
EDIT: HS_TLS_INTUNE

ADSS Service * Certification Service

ADSS Certification Server * ADSS Server (40.87.156.1)

ADSS Certification Service Profile * adss:certification:profile:012

Certificate Purpose TLS Client Authentication

Certificate Enrolment * Device Enrolments

Device Enrolments * Microsoft Intune SCEP ×

Certification profile will be used to support selected Device Enrolment Protocol (s)

Microsoft Intune SCEP Connector * HS_Intune ([redacted].onmicrosoft.com)

□ Microsoft Intune SCEP Device Certificate

4. The Details page will display, these values are only editable if the ADSS Server Certification Profile Allows, if editable set the following, click >:
   - Key Algorithm

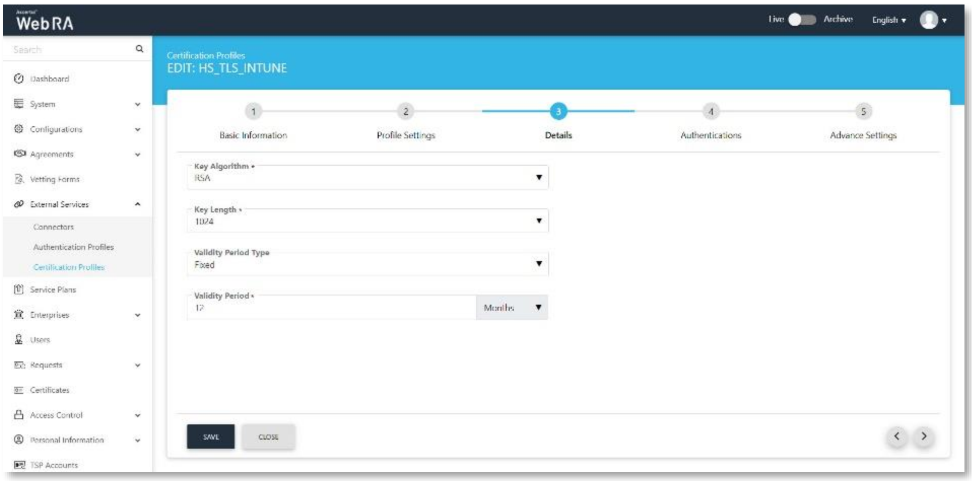
   Key Algorithm that will be used to generate the key pair in the smart card/token. This configuration is coming from the ADSS Server so it cannot be changed.

- Key Length

Key Length that will be used to generate the key pair in the smart card/token. This configuration is coming from the ADSS Server so it cannot be changed.

- Validity Period Type
  - Validity period type can be configured as a Fixed to restrict the enterprise user to change the certificate validity or it can be set as Custom if enterprise RAO allow an enterprise user to set validity period while creating a certificate request.
  - These Fixed and Custom values can only be used on ADSS Web RA admin, if the selected ADSS Certification profile has set over ridable option in certification profile. It will be shown as fixed validity period type otherwise.
- Validity Period

Set the certificate validity period.



EDIT: HS_TLS_INTUNE

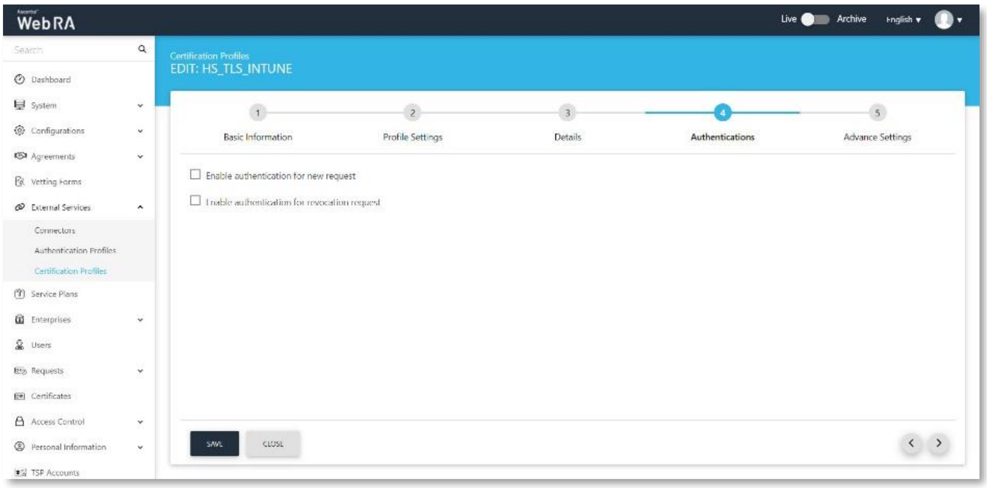
Key Algorithm *: RSA

Key Length *: 1024

Validity Period Type: Fixed

Validity Period *: 12 Months

5. The Authentications page will display. Accept the details, click >

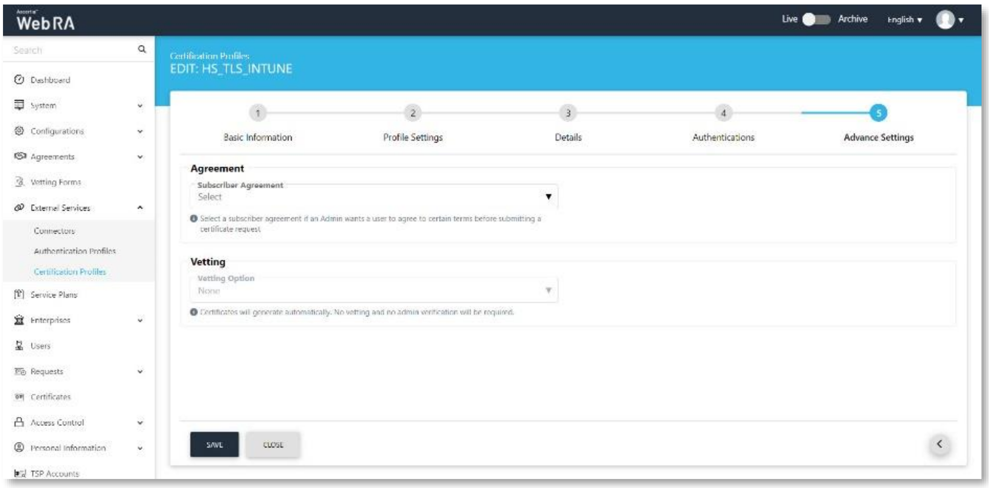


EDIT: HS_TLS_INTUNE

☐ Enable authentication for new request

☐ Enable authentication for revocation request

6. The Advance Settings page will display, accept the default, click Create.



Certification Profiles

EDIT: HS_TLS_INTUNE

Agreement

Subscriber Agreement: Select ▾

Select a subscriber agreement if an Admin wants a user to agree to certain terms before submitting a certificate request

Vetting

Vetting Option: None ▾

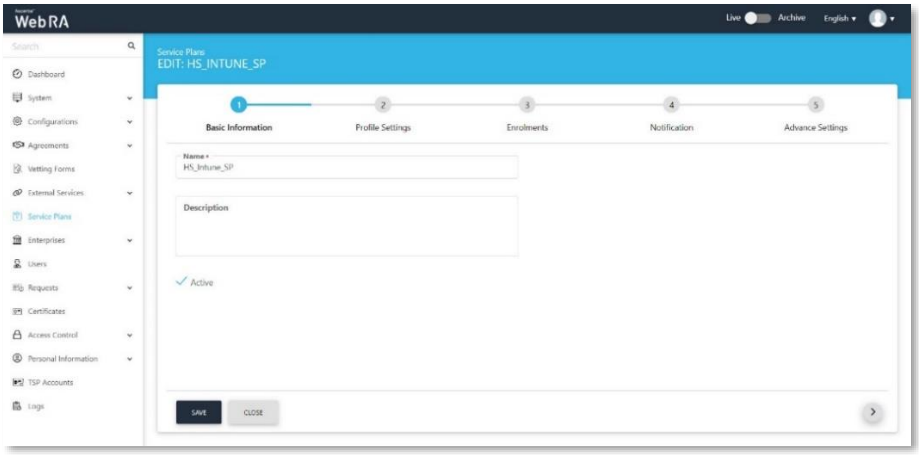
Certificates will generate automatically. No vetting and no admin verification will be required.

7. Repeat this process for any other certificate templates that are required.

5.1.9 Configure a Service Plan

ADSS Web RA Server uses service plans to govern which services and features are available to a given enterprise. This section provides example steps on how to create a basic service plan that will enable the issuance of certificates for Microsoft Intune SCEP. For a detailed reference on service plan settings, please refer to the ADSS Web RA Server product documentation.

1. Expand Service Plans click +
2. The Basic Information page will display, enter a name, select the Active check box, and click >.



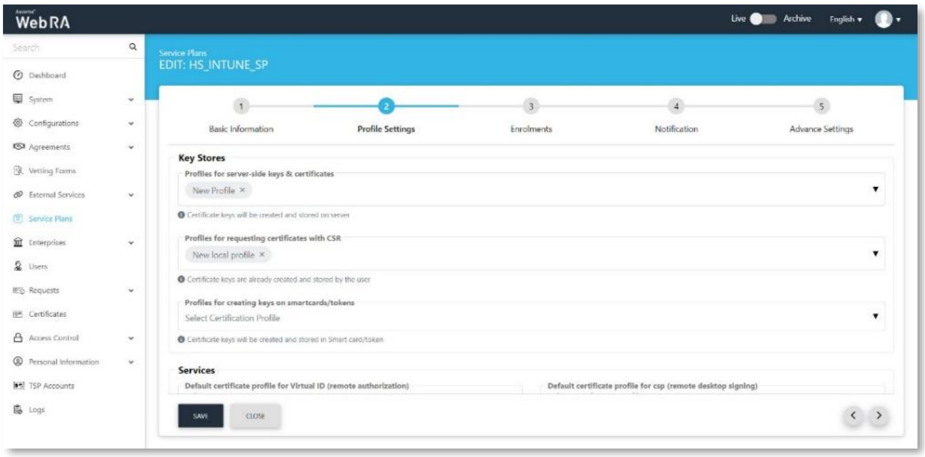
Service Plans
EDIT: HS_INTUNE_SP

Name *: HS_Intune_SP

Description

✓ Active

3. The Profile Settings page will display. Click the Profile to create certificates for Intune SCEP and select the profile created in step 5.1.7, repeat for Profile to create certificates for SCEP , click >.



Service Plans
EDIT: HS_INTUNE_SP

Key Stores

Profiles for server-side keys & certificates: New Profile ×

Certificate keys will be created and stored on server

Profiles for requesting certificates with CSR: New local profile ×

Certificate keys are already created and stored by the user

Profiles for creating keys on smartcards/tokens: Select Certification Profile

Certificate keys will be created and stored in Smart card/token

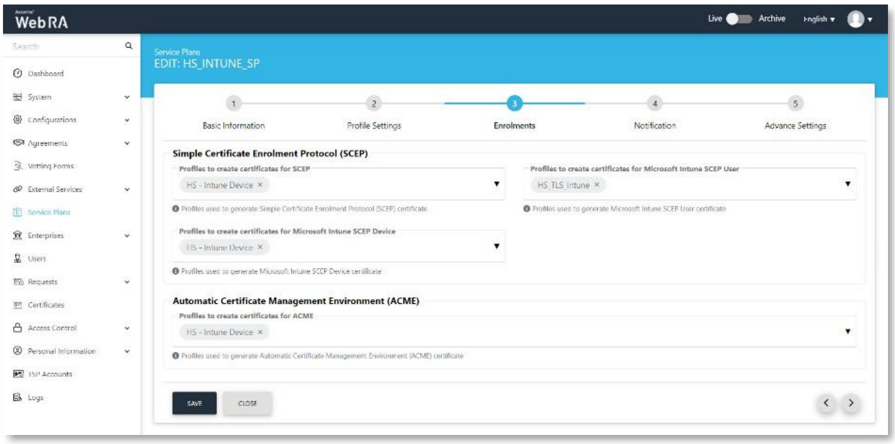
Services

Default certificate profile for Virtual ID (remote authorization)

Default certificate profile for csp (remote desktop signing)

4. The Enrolments page will display.
5. This page consists of the different protocols that ADSS Web RA supports. Under the Simple Certificate Enrolment Protocol (SCEP) section, there are three types of profiles:

Profile to create certificates for SCEP	Configure this profile for SCEP certificates
Profile to create certificates for Microsoft Intune SCEP User	Configure this profile for user-based certificates
Profile to create certificates for Microsoft Intune SCEP Device	Configure this profile for device-based certificates



Service Plans
EDIT: HS_INTUNE_SP

Simple Certificate Enrolment Protocol (SCEP)

Profiles to create certificates for SCEP: HS - Intune Device ×
Profiles used to generate Simple Certificate Enrolment Protocol (SCEP) certificate

Profiles to create certificates for Microsoft Intune SCEP User: HS TLS Intune ×
Profiles used to generate Microsoft Intune SCEP User certificate

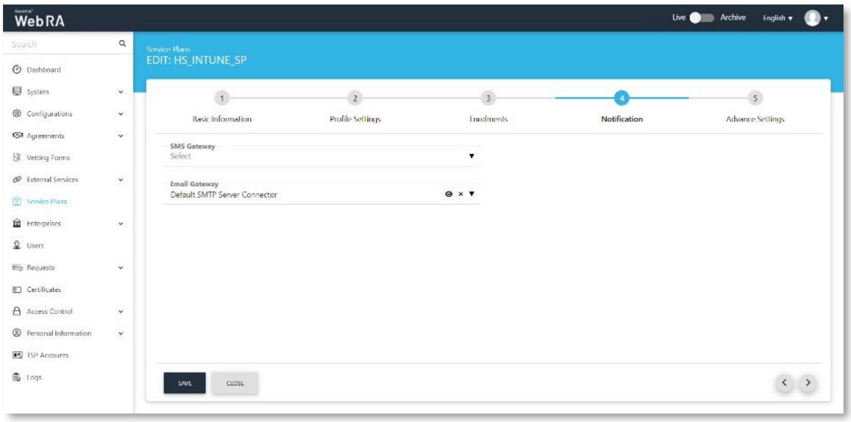
Profiles to create certificates for Microsoft Intune SCEP Device: HS - Intune Device ×
Profiles used to generate Microsoft Intune SCEP Device certificate

Automatic Certificate Management Environment (ACME)

Profiles to create certificates for ACME: HS - Intune Device ×
Profiles used to generate Automatic Certificate Management Environment (ACME) certificate

6. Notifications page will display, enable the notification providers you require for user notifications to be sent, click >.

SMS Gateway	SMS Gateway connector to receive OTP via SMS.
Email Gateway	SMTP connector to receive email notifications.

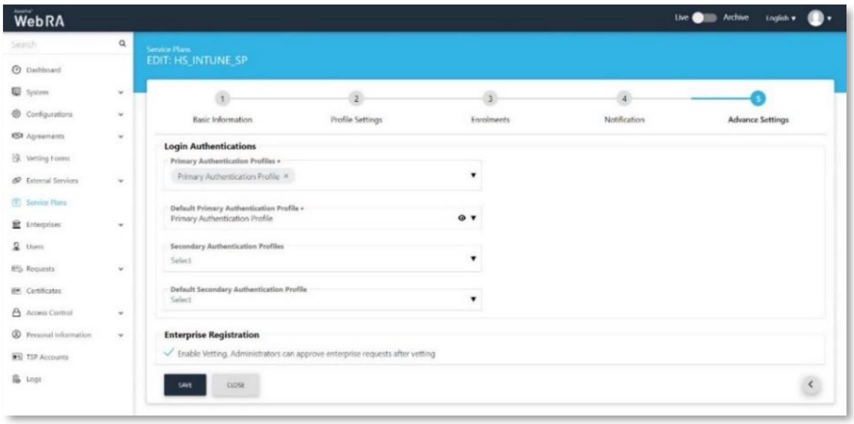


Service Plans
EDIT: HS_INTUNE_SP

SMS Gateway: Select

Email Gateway: Default SMTP Server Connector

7. The Advance Settings page will display, ADSS Web RA Server provides primary and secondary authentication profiles. “Primary Authentication Profiles” are used to control how a user authenticates to Web RA to access the user portal. “Secondary Authentication Profiles” are used when an enterprise wishes to use an additional separate authentication mechanism to authorise an action, such as certificate rekey or revocation.



Service Plans
EDIT: HS_INTUNE_SP

Login Authentications

Primary Authentication Profiles *: Primary Authentication Profile ×

Default Primary Authentication Profile *: Primary Authentication Profile

Secondary Authentication Profiles: Select

Default Secondary Authentication Profile: Select

Enterprise Registration

✓ Enable Vetting, Administrators can approve enterprise requests after vetting

5.1.10 Create an Enterprise

ADSS Web RA Server is a multi-tenanted product that enables different organisations or different departments to be created, each have their own administrative users that can create and manage user invites, and user and device certificates. This section provides steps to create an enterprise that will be used to issue and manager digital certificates for Microsoft Intune SCEP.

1. Access Web RA administration as an administrator with permissions to create enterprises, navigate to Enterprises > Requests click on +.
2. The Organisation Information page will display, provide the following information, click >.

- Legal Name

Legal Name is the official name of the organisation under which the organization is registered with the government and it is the name that is used when submitting tax to the government e.g. Ascertia Limited.

- Assumed Name

Assumed Name could be the short hand name of the organisation that is commonly used e.g. Ascertia.

- Organisation Phone Number

Official phone number of the organisation that is registered in the government documents.

- Address

Complete address of the organisation as it was provided to government at the time of company registration.

The following fields should be filled as part of Address:

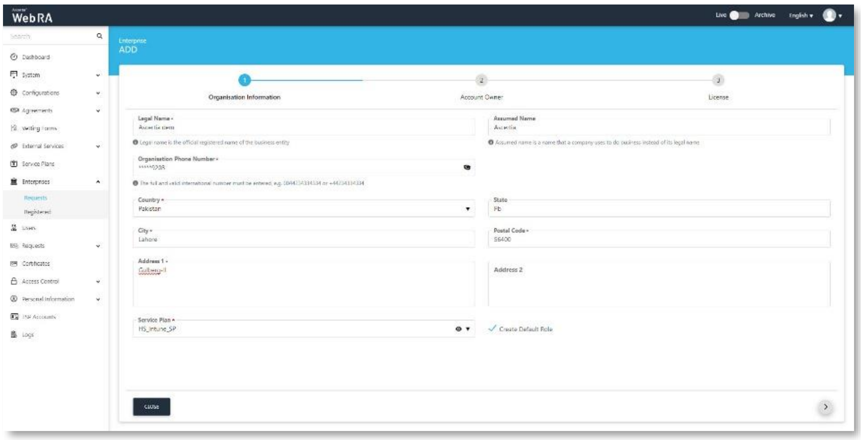
- ○ Country
- ○ State
- ○ City
- ○ Postal Code
- ○ Address 1
- ○ Address 2

- Service Plan

Select a service plan for this enterprise that you created for Microsoft Intune SCEP.

- Create Default Role

Tick this checkbox to create a default role while creating a new enterprise.



Legal Name *: Ascertia demo
Legal name is the official registered name of the business entity
Assumed Name: Ascertia
Assumed name is a name that a company uses to do business instead of its legal name
Organisation Phone Number *: *****9208
The full and valid international number must be entered, e.g. 00442034334334 or +442034334334
Country *: Pakistan
State: Pb
City *: Lahore
Postal Code *: 56400
Address 1 *: Gulberg-II
Address 2
Service Plan *: HS_Intune_SP
✓ Create Default Role

3. The Account Owner page will display, enter the following information, click >

- Name

Name of the enterprise owner. It could be any representative of the organisation but ideally, it should be the CEO. The enterprise owner should initiate any change requested in the enterprise.

- Email

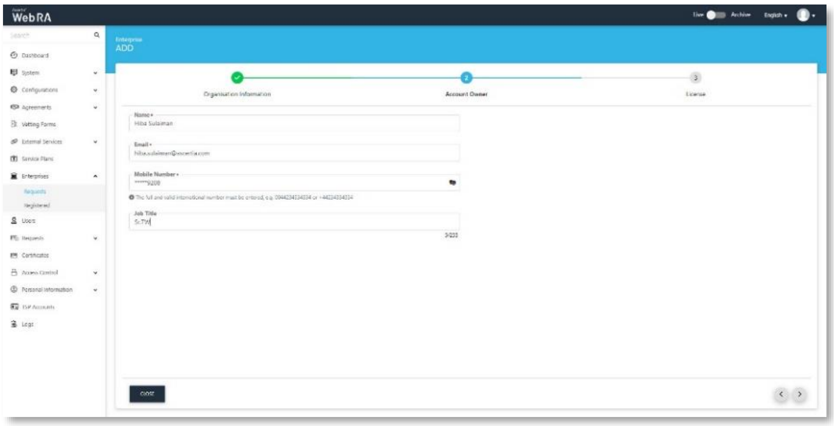
Email address of the enterprise owner. An email will be sent to this email address to create an account on the ADSS Web RA Web.

- Mobile Number

Mobile number of the enterprise owner to send the OTP code if enabled in the profile.

- Job Title

The role of the enterprise owner in his organisation.



Enterprise
ADD

Organisation Information — Account Owner — License

Name *
Hiba Sulaiman

Email *
hiba.sulaiman@ascertia.com

Mobile Number *
*****9200

The full and valid international number must be entered, e.g. 00442343434334 or +442343434334

Job Title
Sr.TW

3/200

4. The License page will display, enter the certificate quota and expiry for the Enterprise, click create.

- Name

Name of the certification profile for which an enterprise wants to use ADSS Web RA to create certificates.

- Unlimited

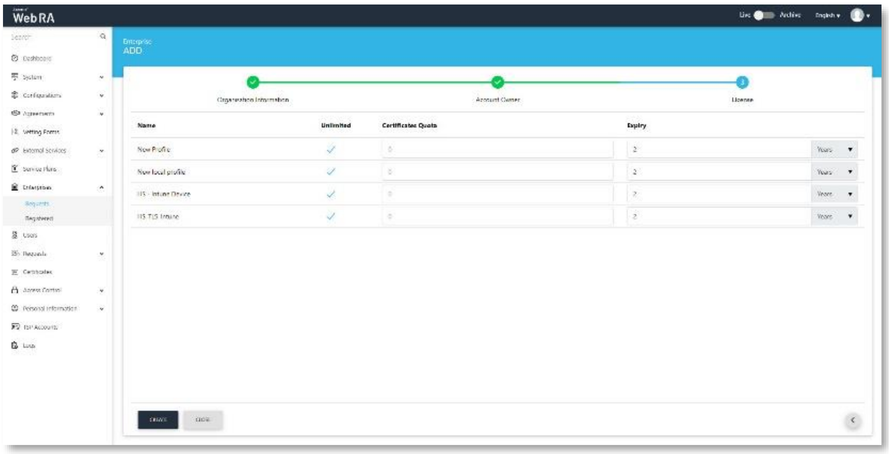
A check box can be used to allow a user to create unlimited certificates. This field will appear only if a user is allowed to create unlimited certificates.

- Certificates Quota

This defines the total number of certificates an enterprise is allowed to generate from ADSS Web RA against each certification profile.

- Expiry

This defines the duration for which these certificates are valid.

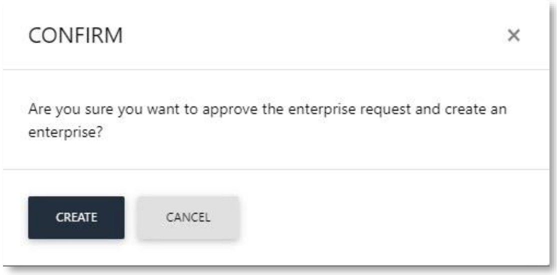


Enterprise
ADD

Organization Information — Account Owner — License

Name	Unlimited	Certificates Quota	Expiry	
New Profile	✓	0	2	Years
New local profile	✓	0	2	Years
HS - Intune Device	✓	0	2	Years
HS TLS Intune	✓	0	2	Years

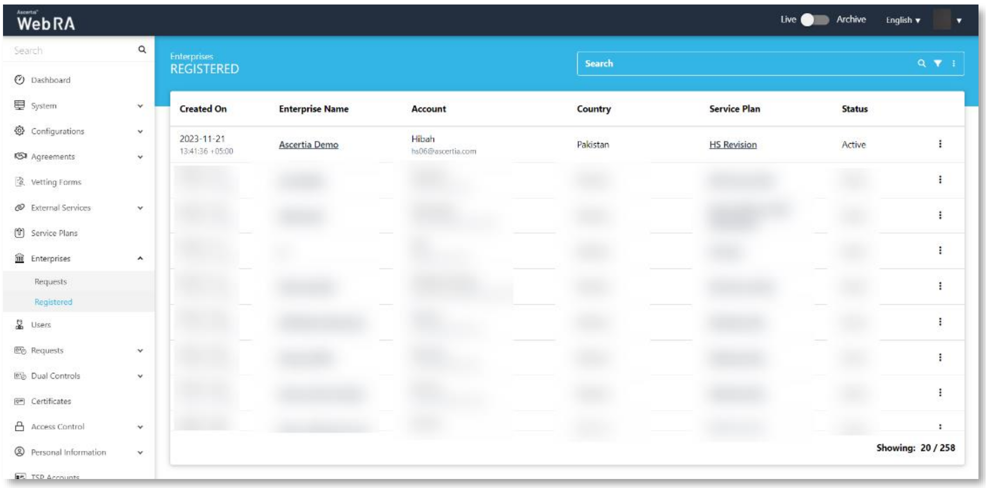
5. A confirmation dialog will display, click Yes to create the enterprise.



CONFIRM

Are you sure you want to approve the enterprise request and create an enterprise?

6. Click Registered from the left menu, your new enterprise will appear.



Enterprises
REGISTERED

Created On	Enterprise Name	Account	Country	Service Plan	Status
2023-11-21 13:41:36 +05:00	Ascertia Demo	Hibah hs06@ascertia.com	Pakistan	HS Revision	Active

Showing: 20 / 258

7. Click on the enterprise name, you will be directed to the enterprise management screen. Expand Users > User Invitations.

Information

- Name

Enter name of the user you wish to invite to the enterprise.

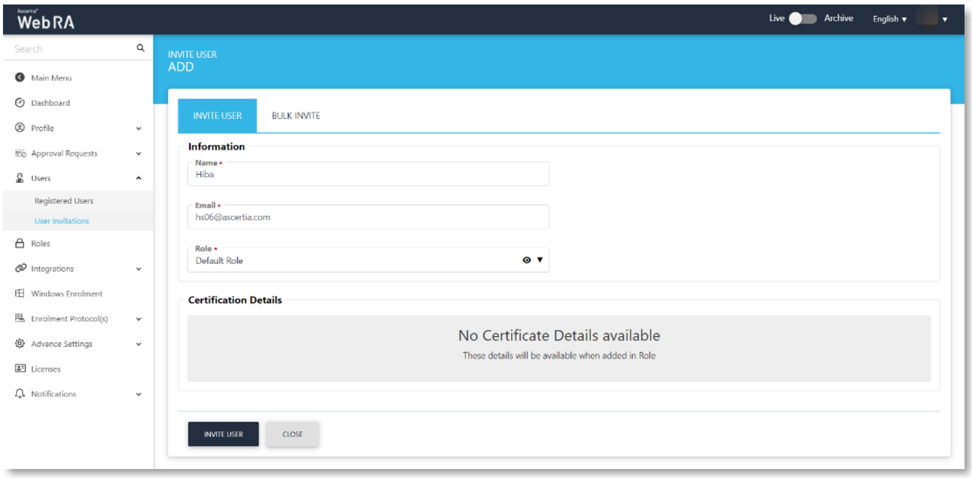
- Email

Enter email of the user you wish to invite to the enterprise.

- Role

Select a role for the user.

Click Invite User.



INVITE USER
ADD

Information

Name * Hiba

Email * hs06@ascertia.com

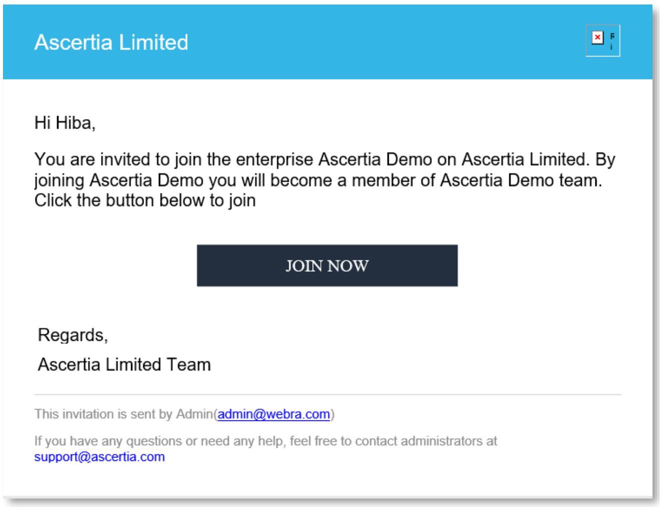
Role * Default Role

Certification Details

No Certificate Details available

These details will be available when added in Role

8. An email will be sent to the user on the above configured email address. (As displayed below) Click Join Now.



Ascertia Limited

Hi Hiba,

You are invited to join the enterprise Ascertia Demo on Ascertia Limited. By joining Ascertia Demo you will become a member of Ascertia Demo team. Click the button below to join

Regards,

Ascertia Limited Team

This invitation is sent by Admin(admin@webra.com)

If you have any questions or need any help, feel free to contact administrators at support@ascertia.com

9. The user will be redirected to the ADSS Web RA web portal’s account activation screen. Enter the details:

- Email

Email of the user to register on the Web portal.

- Mobile Number

Mobile number of the user.

- Password

Set a password for the login email.

- Confirm Password

Confirm password for the login email.

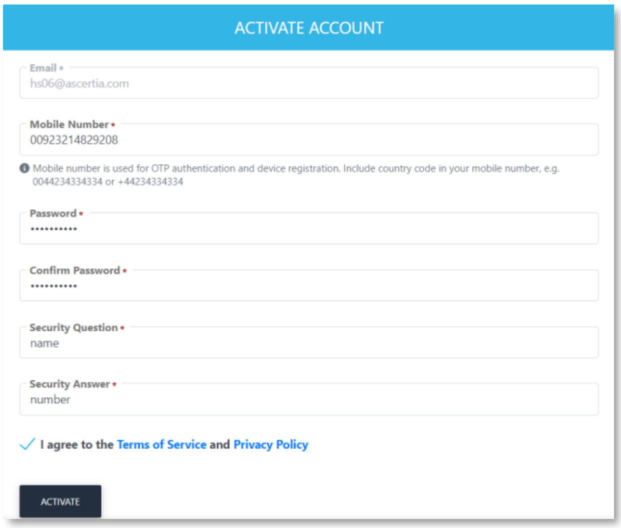
- Security Question

Set a security question for password recovery

- Security Answer
- Set a security answer for password recovery

Select I agree to the Terms of Service and Privacy Policy.

Click Activate.



ACTIVATE ACCOUNT

Email *
hs06@ascertia.com

Mobile Number *
00923214829208

Mobile number is used for OTP authentication and device registration. Include country code in your mobile number, e.g. 0044234334334 or +44234334334

Password *
••••••••••

Confirm Password *
••••••••••

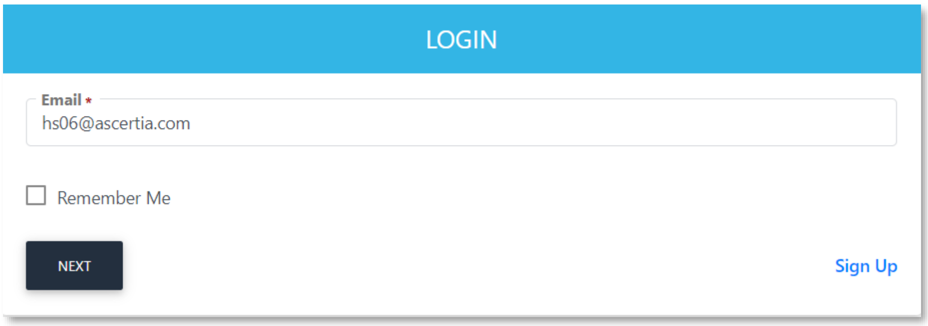
Security Question *
name

Security Answer *
number

✓ I agree to the Terms of Service and Privacy Policy

ACTIVATE

10. The user will now be directed to the Login screen, enter the user email and click Next.



LOGIN

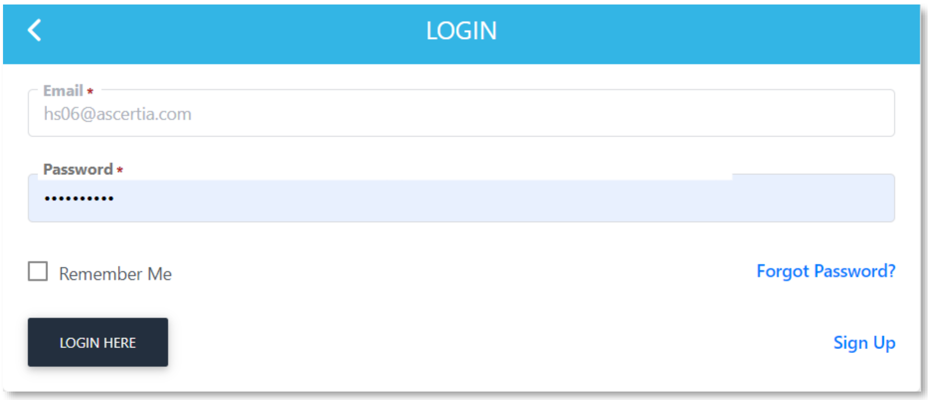
Email *
hs06@ascertia.com

□ Remember Me

NEXT

Sign Up

11. Enter the password and click Login Here.



LOGIN

Email *
hs06@ascertia.com

Password *
••••••••••

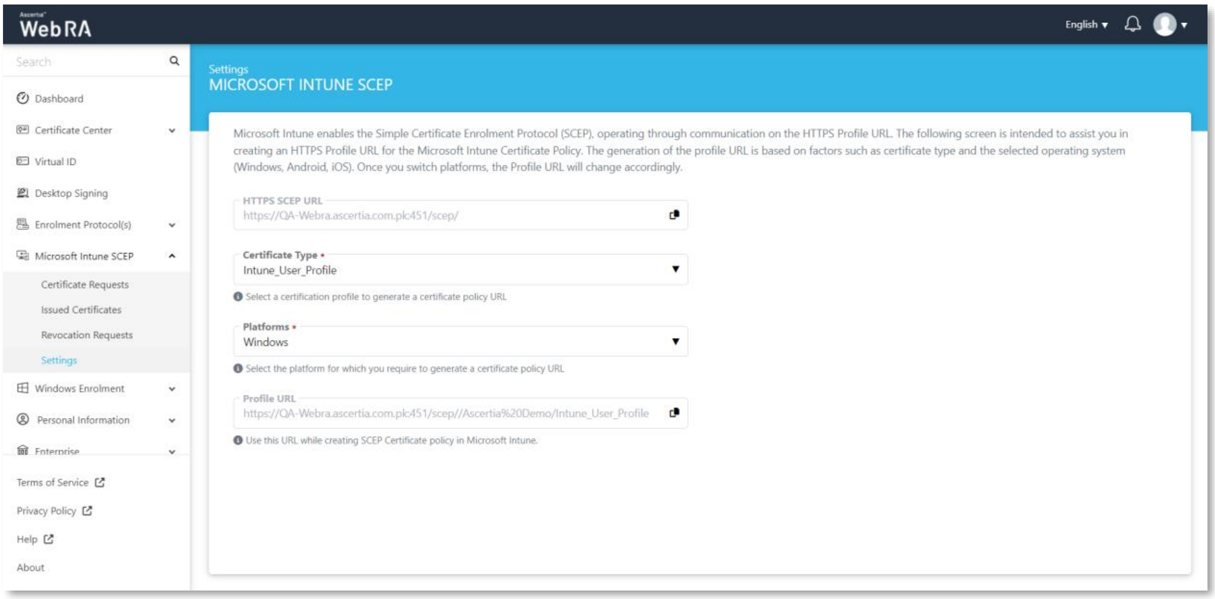
□ Remember Me

Forgot Password?

LOGIN HERE

Sign Up

12. The user will be logged in to the ADSS Web RA web portal. Expand Microsoft Intune SCEP > Settings to generate the SCEP Profile URL that will be required while creating SCEP profile in Microsoft Intune.



Settings
MICROSOFT INTUNE SCEP

Microsoft Intune enables the Simple Certificate Enrolment Protocol (SCEP), operating through communication on the HTTPS Profile URL. The following screen is intended to assist you in creating an HTTPS Profile URL for the Microsoft Intune Certificate Policy. The generation of the profile URL is based on factors such as certificate type and the selected operating system (Windows, Android, iOS). Once you switch platforms, the Profile URL will change accordingly.

HTTPS SCEP URL: https://QA-Webra.ascertia.com.pk:451/scep/

Certificate Type *: Intune_User_Profile

Select a certification profile to generate a certificate policy URL

Platforms *: Windows

Select the platform for which you require to generate a certificate policy URL

Profile URL: https://QA-Webra.ascertia.com.pk:451/scep//Ascertia%20Demo/Intune_User_Profile

Use this URL while creating SCEP Certificate policy in Microsoft Intune.

- Certificate Type

Select the certificate profile to generate a certificate policy URL, i.e. user, user device, or device.

- Platforms

Select the platform for which you require to generate a certificate policy URL i.e. Android, iOS or Windows.

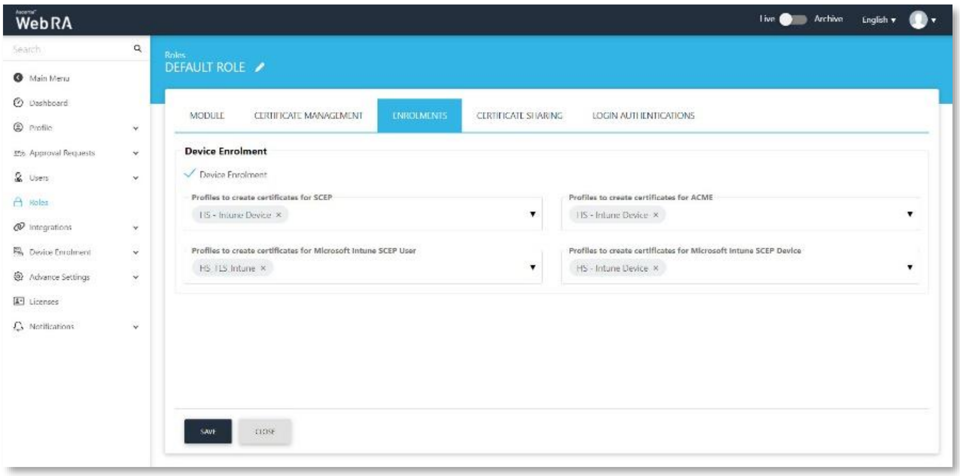
- Profile URL

Once you select the certificate type and platform, a URL will be generated. You will be required to use this URL while creating SCEP certificate policy in Microsoft Intune.

5.1.11 Edit the Enterprise Default Role

Microsoft Intune users are automatically registered in the default enterprise role during the auto-enrolment of certificates. This section includes the steps to control which certificates will be displayed to a user in the ADSS Web RA Server User Portal.

1. Access ADSS Web RA administration as an administrator with permissions to edit roles, expand Enterprises > Registered > select the Enterprise Name > Manage> Roles > click the ⋮ to edit the Default Role > Enrolments.
2. Select the Enrolment Protocol (s) check box and select the certificate profiles from the various enrolment protocol (s) available.
3. Click Save when complete.



Device Enrolment

✓ Device Enrolment

Profiles to create certificates for SCEP: HS - Intune Device ×

Profiles to create certificates for ACME: HS - Intune Device ×

Profiles to create certificates for Microsoft Intune SCEP User: HS TLS Intune ×

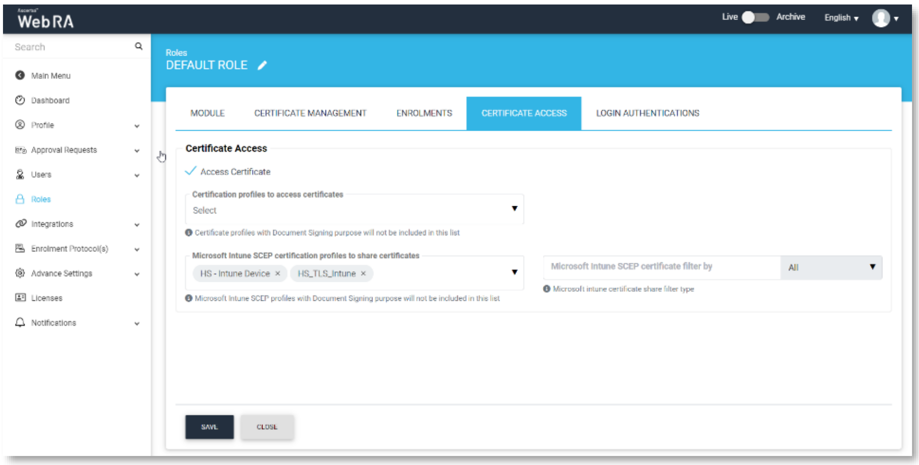
Profiles to create certificates for Microsoft Intune SCEP Device: HS - Intune Device ×

Users can access ADSS Web RA admin to manage certificates issued to them by the Intune SCEP enrolment process. The Profiles to create certificates for SCEP drop-down enables Web RA Administrators to define which user profiles a user can access via the Web RA user portal. The Profile to create certificates for ACME drop-down enables Web RA Administrators to define which SCEP profiles a user can access via the Web RA user portal. The Profiles to create certificates for Microsoft Intune SCEP User drop-down enables Web RA Administrators to define which user profiles a user can access via the Web RA user portal. The Profiles to create certificates for Microsoft Intune SCEP Device drop-down enables Web RA Administrators to define which device profiles a user can access via the Web RA user portal.

Certificate Access

1. Select the Access Certificate check box and select certification profiles to access certificates. This drop down allows users to gain access to certificates based on the profiles they configure.
2. Select a Microsoft Intune SCEP certification profiles to share certificates with other users. This setting allows you to configure profiles to share certificates.
3. Microsoft Intune SCEP certificate filter by:

Once configured, this profile will enable you to apply a filter based on elements of a certificate's subject distinguished name (SDNs), these include, all, common name, first name, country, etc. on basis of which certificate requests will appear on the ADSS Web RA web portal, and the user will only be able to manage according to the filters applied here. Once the required filters have been defined, click Save.



Certificate Access

✓ Access Certificate

Certification profiles to access certificates: Select

Certificate profiles with Document Signing purpose will not be included in this list

Microsoft Intune SCEP certification profiles to share certificates: HS - Intune Device × HS_TLS_Intune ×

Microsoft Intune SCEP profiles with Document Signing purpose will not be included in this list

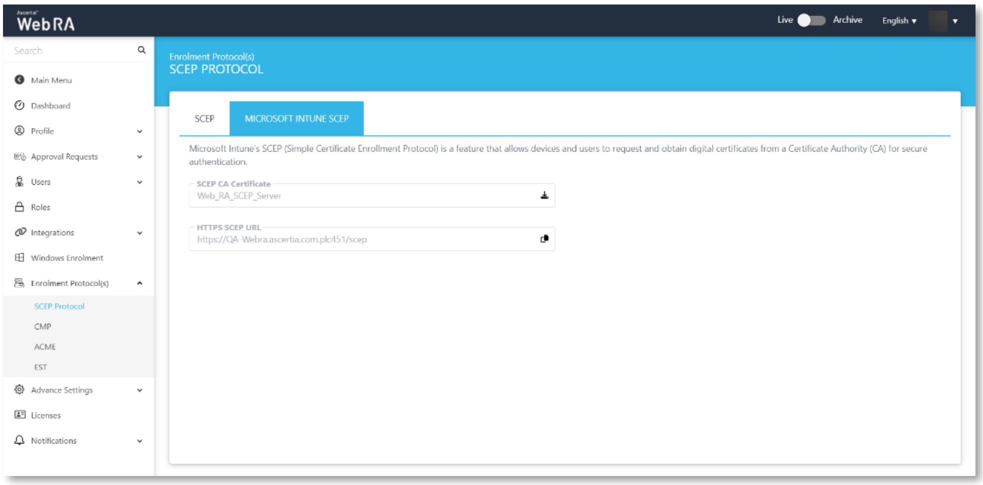
Microsoft Intune SCEP certificate filter by: All

Microsoft intune certificate share filter type

Enrolment Protocol (s)

If the Microsoft Intune SCEP is enabled in the Configurations section in the ADSS Web RA admin portal, then the following section with appear in the Enterprise section under the Enrolment Protocol(s) section.

Access ADSS Web RA administration as an administrator with permissions to edit roles, expand Enterprises > Registered > select the Enterprise Name > Manage> Enrolment Protocol (s) > SCEP Protocol, click the Microsoft Intune SCEP.



Microsoft Intune's SCEP (Simple Certificate Enrollment Protocol) is a feature that allows devices and users to request and obtain digital certificates from a Certificate Authority (CA) for secure authentication.

SCEP CA Certificate: Web_RA_SCEP_Server

HTTPS SCEP URL: https://QA-Webra.ascertia.com.pk:451/scep

You can click on the download button against the SCEP CA Certificate to download the chain of certificates from ADSS Web RA Sever that will be used later to create trusted certificates in Microsoft Intune.

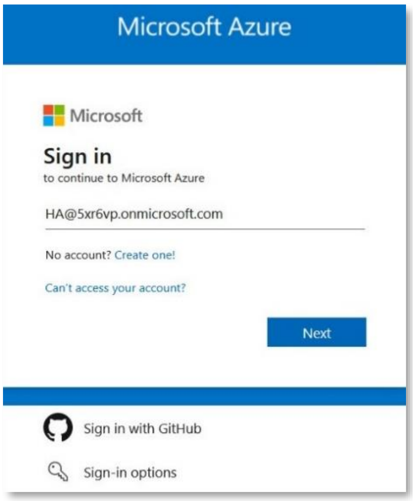
6 Configure Microsoft Intune

The following system and environment pre-requisites need to be fulfilled prior to the configurations of the ADSS Web RA Server Microsoft Intune SCEP.

6.1. Configure Microsoft Intune

Before you begin, you need to configure your Microsoft and secure with two-factor authentication.

1. Login to Microsoft Intune through this link https://endpoint.microsoft.com/#home.
2. Use your Microsoft administrator e.g. HA@5xr6vp.onmicrosoft.com to login. Click Next.



Microsoft Azure

Microsoft

Sign in

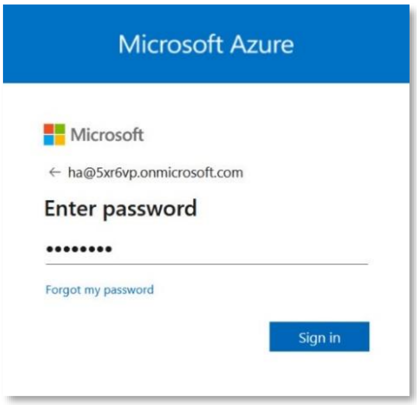
to continue to Microsoft Azure

HA@5xr6vp.onmicrosoft.com

No account? Create one!

Can't access your account?

3. Then enter the password and click Sign In.



Microsoft Azure

Microsoft

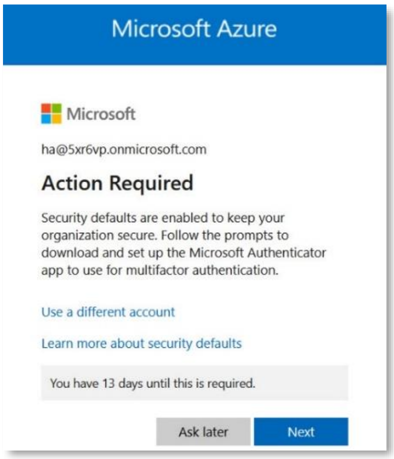
← ha@5xr6vp.onmicrosoft.com

Enter password

••••••••

Forgot my password

4. A security action will be required to set up the Microsoft Authenticator, click Next.



Microsoft Azure

Microsoft

ha@5xr6vp.onmicrosoft.com

Action Required

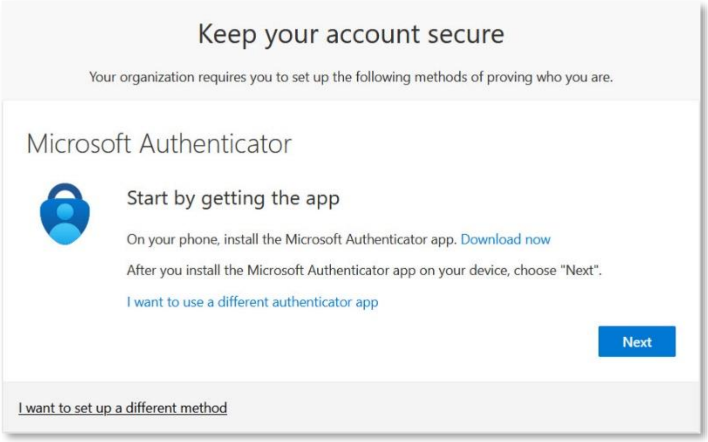
Security defaults are enabled to keep your organization secure. Follow the prompts to download and set up the Microsoft Authenticator app to use for multifactor authentication.

Use a different account

Learn more about security defaults

You have 13 days until this is required.

5. The keep your account safe screen will appear, click Next.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Start by getting the app

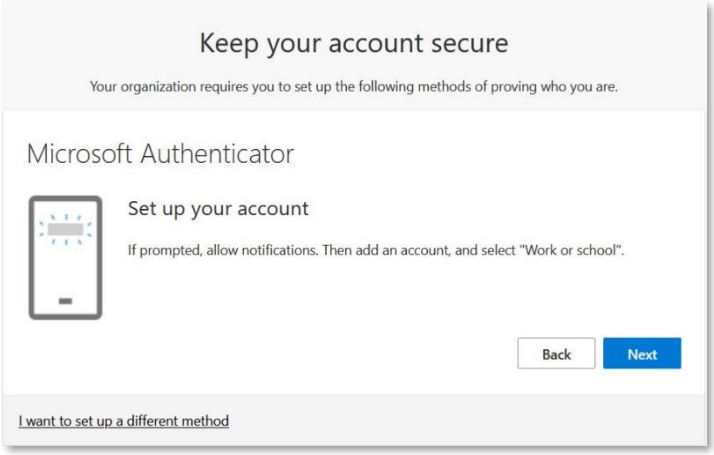
On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

I want to set up a different method

6. To set up the Microsoft Authenticator account, click Next.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

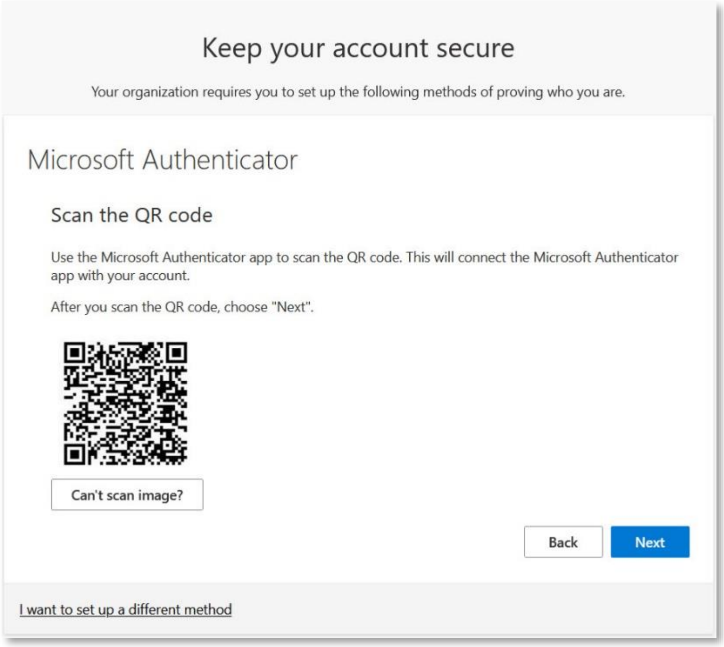
Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

I want to set up a different method

7. Download the Microsoft Authenticator app from the App Store on your mobile device and Scan the QR code appearing on the screen, and click Next.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

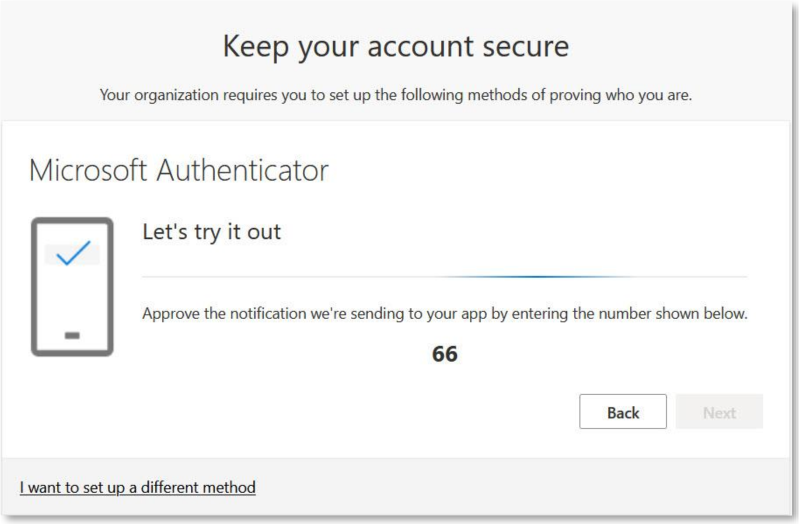
Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

I want to set up a different method

8. Open the Authenticator app on your mobile device and enter the code, e.g. 66.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

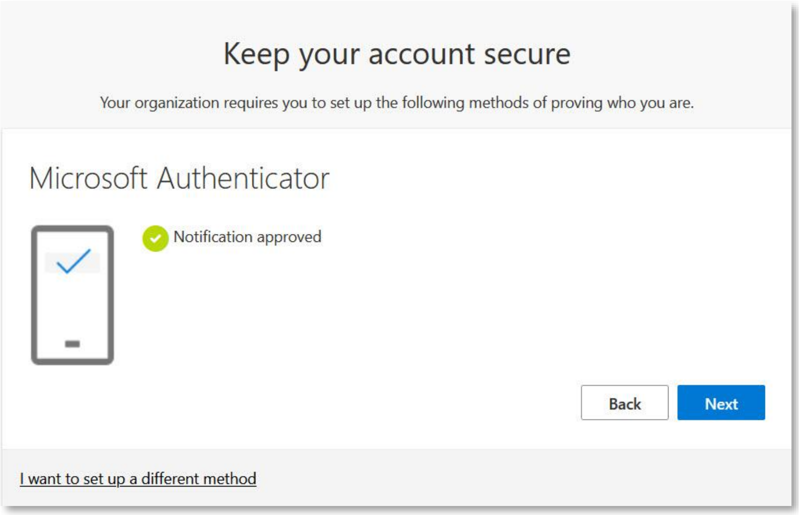
Microsoft Authenticator

Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

66

9. The notification approved message will appear, click Next to proceed.



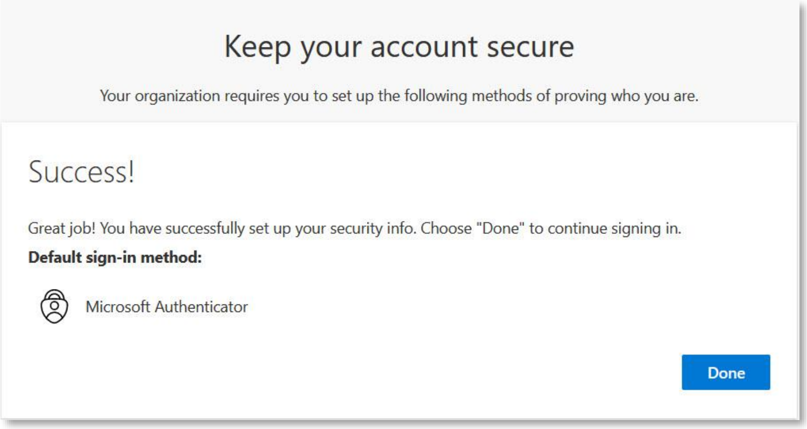
Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Notification approved

10. Once the success message appears, click Done to complete the process.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

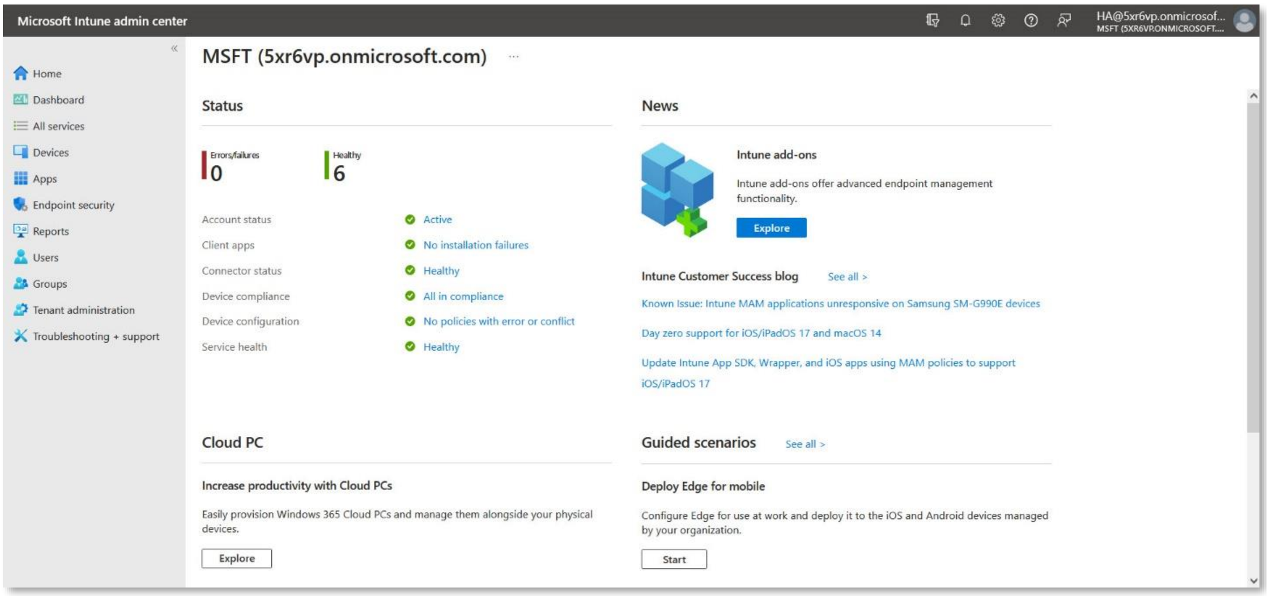
Default sign-in method:

Microsoft Authenticator

6.1.1. Add Intune users in the Microsoft Intune admin center

Follow the steps defined below to configure Microsoft Intune for Certificate Enrolment.

1. After completing the two-factor authentication successfully, you will be directed to the Microsoft Intune admin center.



Account status	Active
Client apps	No installation failures
Connector status	Healthy
Device compliance	All in compliance
Device configuration	No policies with error or conflict
Service health	Healthy

Intune add-ons offer advanced endpoint management functionality.

Known Issue: Intune MAM applications unresponsive on Samsung SM-G990E devices

Day zero support for iOS/iPadOS 17 and macOS 14

Update Intune App SDK, Wrapper, and iOS apps using MAM policies to support iOS/iPadOS 17

Increase productivity with Cloud PCs

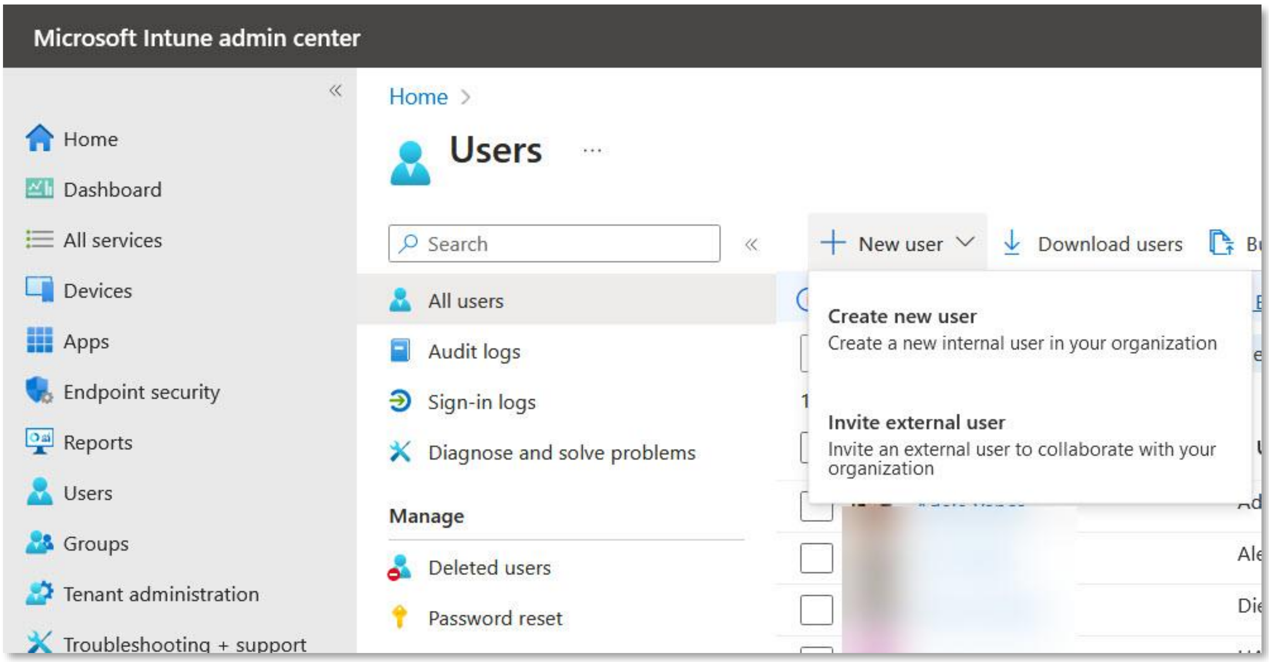
Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Deploy Edge for mobile

Configure Edge for use at work and deploy it to the iOS and Android devices managed by your organization.

2. Select Users from the left panel.

Then click New user > Create new user from the drop down.



Create new user
Create a new internal user in your organization

Invite external user
Invite an external user to collaborate with your organization

3. Provide the following user details in the Basics tab:

- User principal name

Universal principle name (UPN) stored in Azure Active Directory used to access the service, e.g: Hiba.Sulaiman.

- Mail nickname

The Derive from user principal name is checked by default.

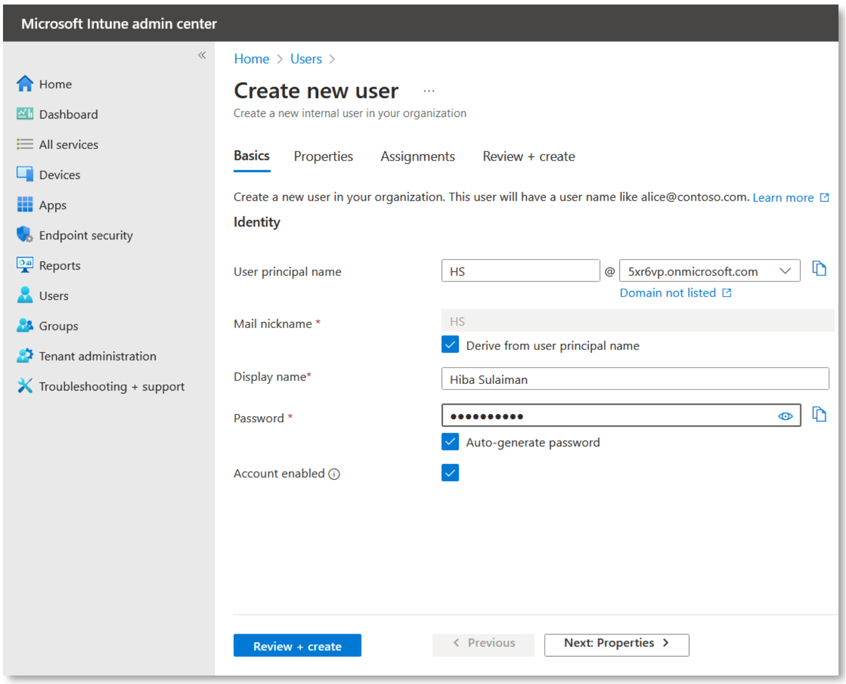
- Display name

Set any name e.g. Hiba Sulaiman.

- Password

You can opt for an auto-generated password or create one manually.
The auto-generate password is checked by default, copy and save it for later use.

- The Account enabled is checked by default.



Create new user

Create a new internal user in your organization

Create a new user in your organization. This user will have a user name like alice@contoso.com. Learn more

Identity

User principal name: HS @ 5xr6vp.onmicrosoft.com

Mail nickname *: HS

☑ Derive from user principal name

Display name*: Hiba Sulaiman

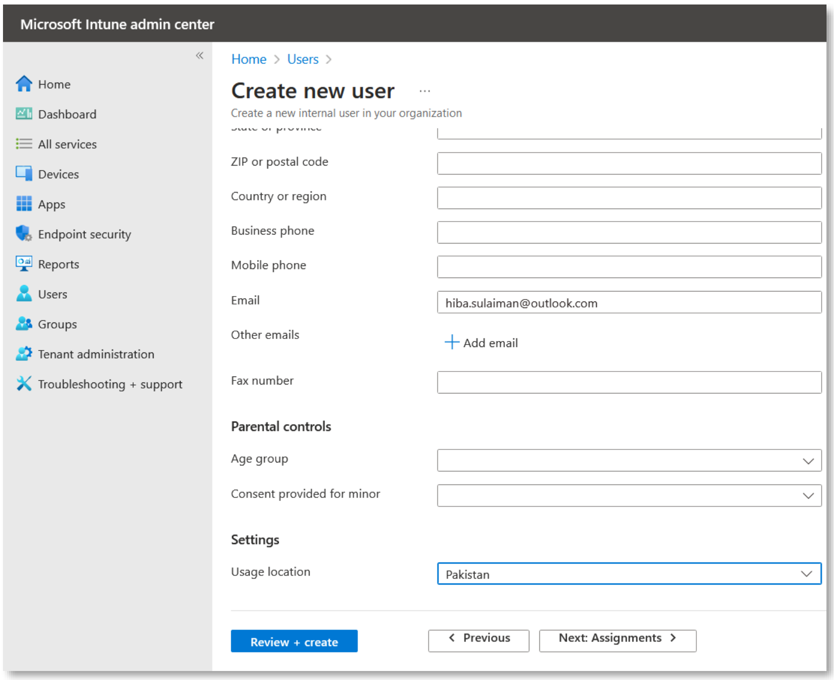
Password *: ••••••••••

☑ Auto-generate password

Account enabled: ☑

4. Click Next: Properties >.

- Enter email.
- Under the Settings > set Usage location. (This is required to assign license to a user in the next steps).



Create new user

Create a new internal user in your organization

State or province

ZIP or postal code

Country or region

Business phone

Mobile phone

Email: hiba.sulaiman@outlook.com

Other emails

Fax number

Parental controls

Age group

Consent provided for minor

Settings

Usage location: Pakistan

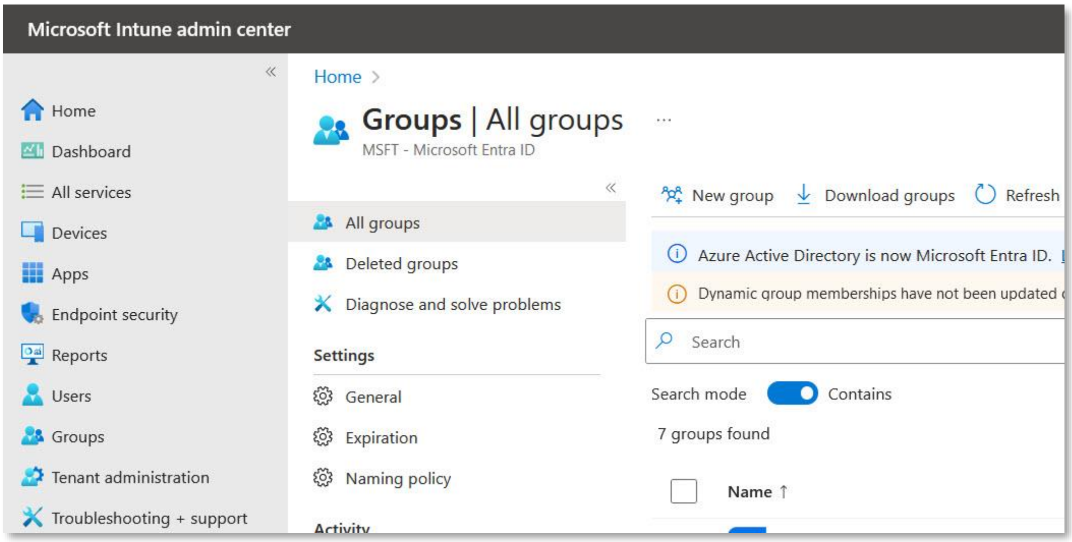
5. Click Review + Create.

The user will be added successfully. Click the Refresh button if it does not appear in the list.

6.1.2. Add Groups

Use the following steps to create a new group.

1. Select Groups from the left panel and then click New group.



Azure Active Directory is now Microsoft Entra ID.

Dynamic group memberships have not been updated

7 groups found

2. Provide the following group details:

- Specify a Group type

e.g. Microsoft 365.

- Set a Group name

e.g. TW_Group.

- Provide a Group description

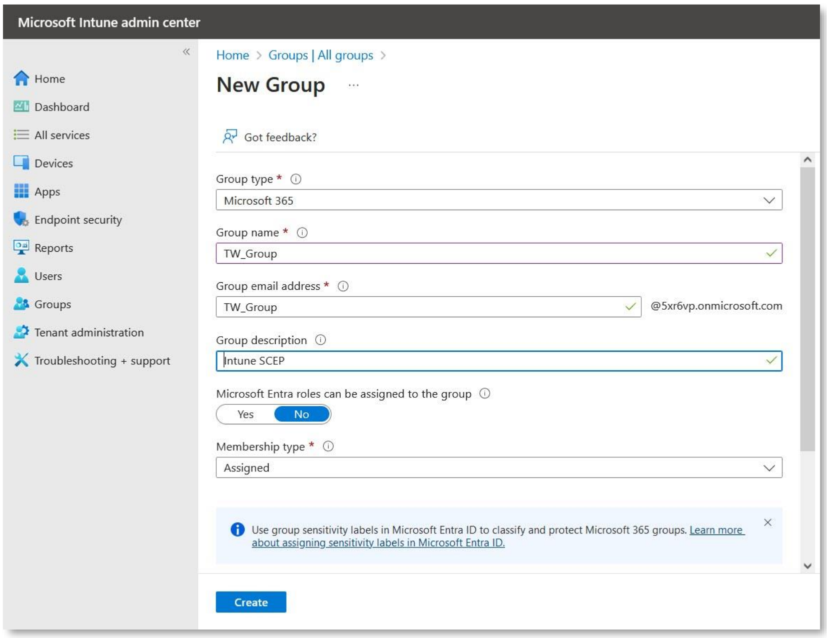
This should be specific and should include information so others know what the group is for, e.g. Intune SCEP.

- Select Azure AD roles can be assigned to the group

No.

- Membership type

Administrators manually assign users or devices to this group, and manually remove users or devices, e.g. Assigned.



Group type * Microsoft 365

Group name * TW_Group

Group email address * TW_Group @5xr6vp.onmicrosoft.com

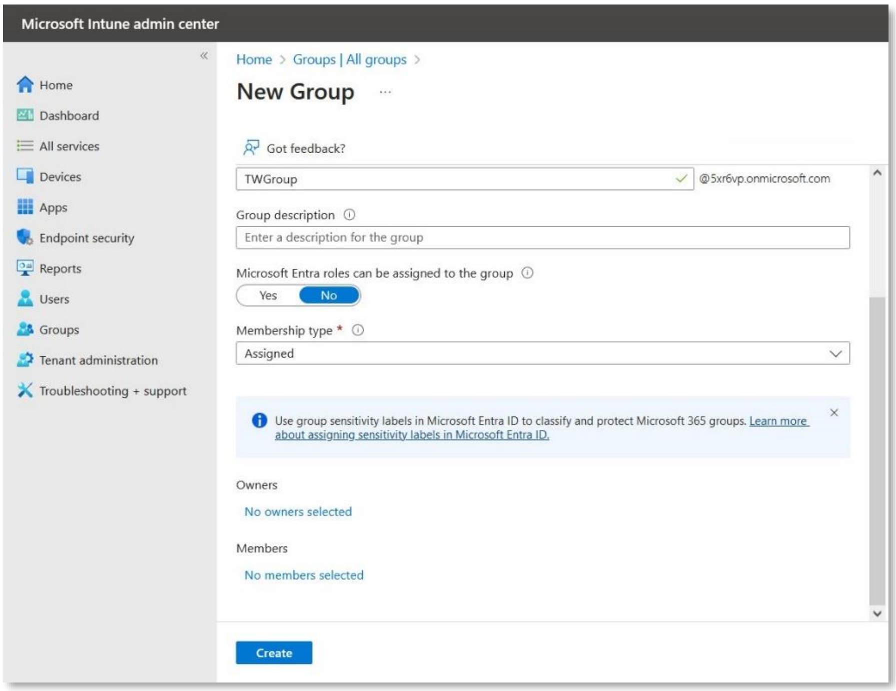
Group description Intune SCEP

Microsoft Entra roles can be assigned to the group Yes [✓ No]

Membership type * Assigned

Use group sensitivity labels in Microsoft Entra ID to classify and protect Microsoft 365 groups. Learn more about assigning sensitivity labels in Microsoft Entra ID.

3. Scroll below and under the Owners tab click on No owners selected.



New Group

TWGroup @5xr6vp.onmicrosoft.com

Group description ⓘ

Enter a description for the group

Microsoft Entra roles can be assigned to the group ⓘ

Yes [✓ No]

Membership type * ⓘ

Assigned

Use group sensitivity labels in Microsoft Entra ID to classify and protect Microsoft 365 groups. Learn more about assigning sensitivity labels in Microsoft Entra ID.

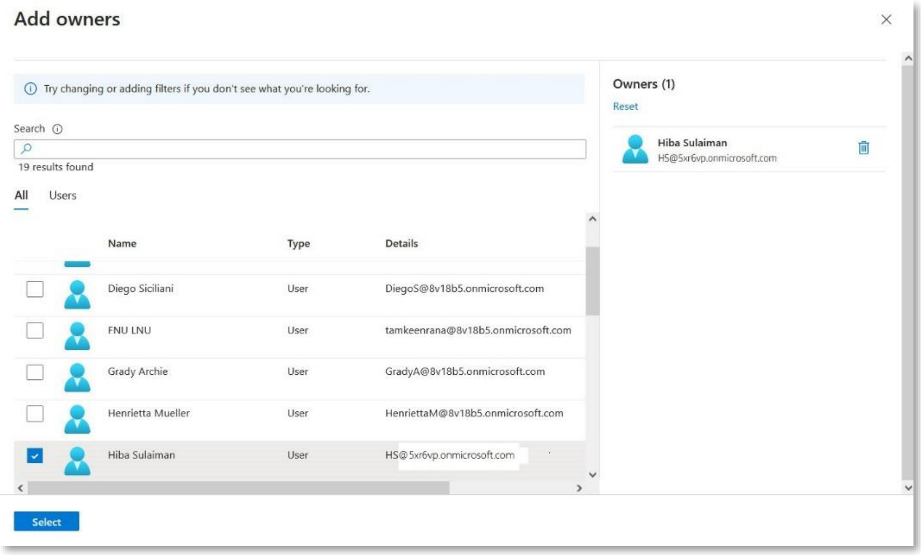
Owners

No owners selected

Members

No members selected

4. On the Add owners screen, select you user e.g. Hiba Sulaiman from the list and click Select.



ⓘ Try changing or adding filters if you don't see what you're looking for.

Search ⓘ

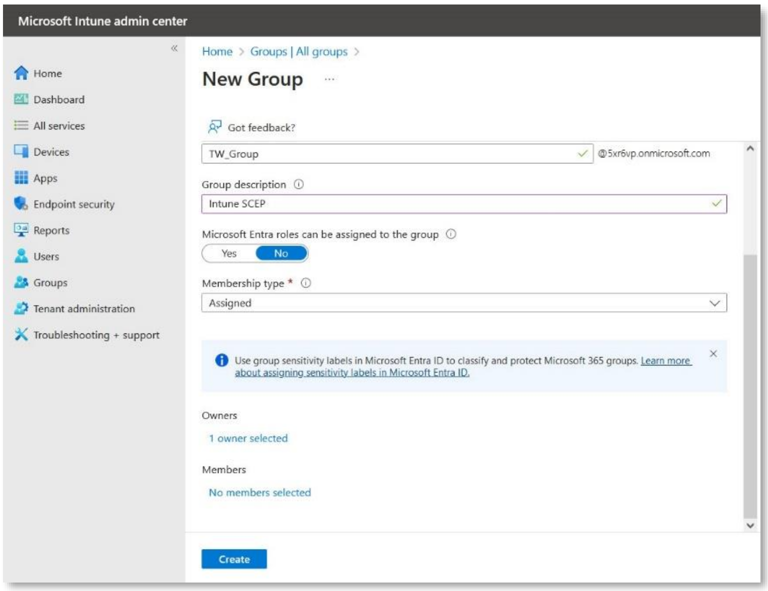
19 results found

	Name	Type	Details
□	Diego Siciliani	User	DiegoS@8v18b5.onmicrosoft.com
□	FNU LNU	User	tamkeenrana@8v18b5.onmicrosoft.com
□	Grady Archie	User	GradyA@8v18b5.onmicrosoft.com
□	Henrietta Mueller	User	HenriettaM@8v18b5.onmicrosoft.com
☑	Hiba Sulaiman	User	HS@5xr6vp.onmicrosoft.com

Owners (1)

Hiba Sulaiman
HS@5xr6vp.onmicrosoft.com

5. You will returned to the New Group screen, and 1 owner selected will be updated. From the Members tab, click No member selected to select members you want to allow to this group.



TW_Group @5xr6vp.onmicrosoft.com

Group description: Intune SCEP

Microsoft Entra roles can be assigned to the group: Yes [✓ No]

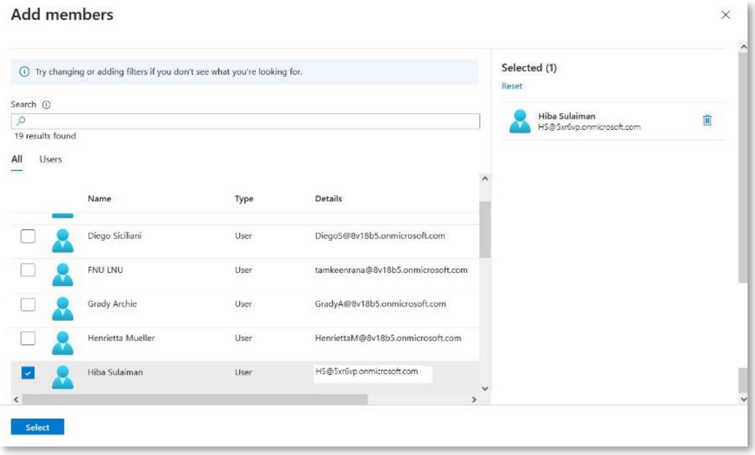
Membership type *: Assigned

Use group sensitivity labels in Microsoft Entra ID to classify and protect Microsoft 365 groups. Learn more about assigning sensitivity labels in Microsoft Entra ID.

Owners: 1 owner selected

Members: No members selected

6. The Add Members screen will appear. Select the user from the list e.g. Hiba Sulaiman and then click Select.



Try changing or adding filters if you don't see what you're looking for.

Search

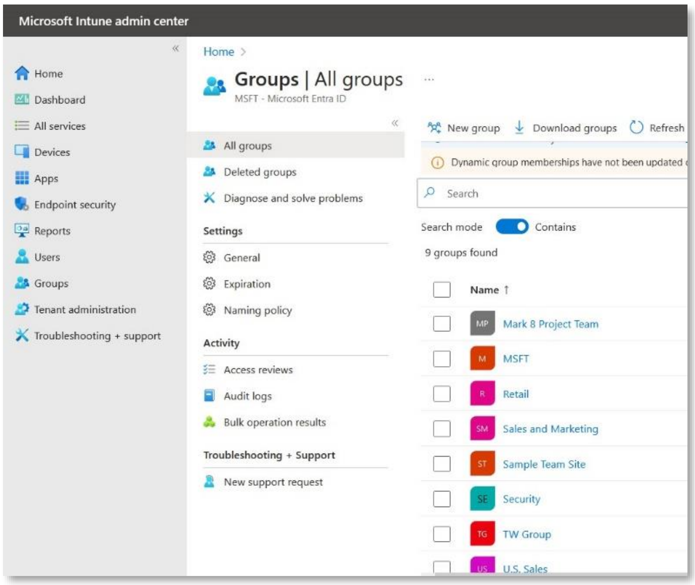
19 results found

	Name	Type	Details
□	Diego Siciliani	User	DiegoS@8v18b5.onmicrosoft.com
□	FNU LNU	User	tamkeenrana@8v18b5.onmicrosoft.com
□	Grady Archie	User	GradyA@8v18b5.onmicrosoft.com
□	Henrietta Mueller	User	HenriettaM@8v18b5.onmicrosoft.com
☑	Hiba Sulaiman	User	HS@5xr6vp.onmicrosoft.com

Hiba Sulaiman
HS@5xr6vp.onmicrosoft.com

7. Click Create to add the new group. Your group is shown in the list.

If it does not appear, click Refresh button and your group will be listed as shown in the screen below. Click your group e.g. TW Group.



Dynamic group memberships have not been updated

Search mode: Contains

9 groups found

	Name ↑
□	MP Mark 8 Project Team
□	M MSFT
□	R Retail
□	SM Sales and Marketing
□	ST Sample Team Site
□	SE Security
□	TG TW Group
□	US U.S. Sales

You must assign each user an Intune license or Group before users can enrol their devices in Intune.

6.1.3. Assign an Intune license in the Microsoft Intune admin center

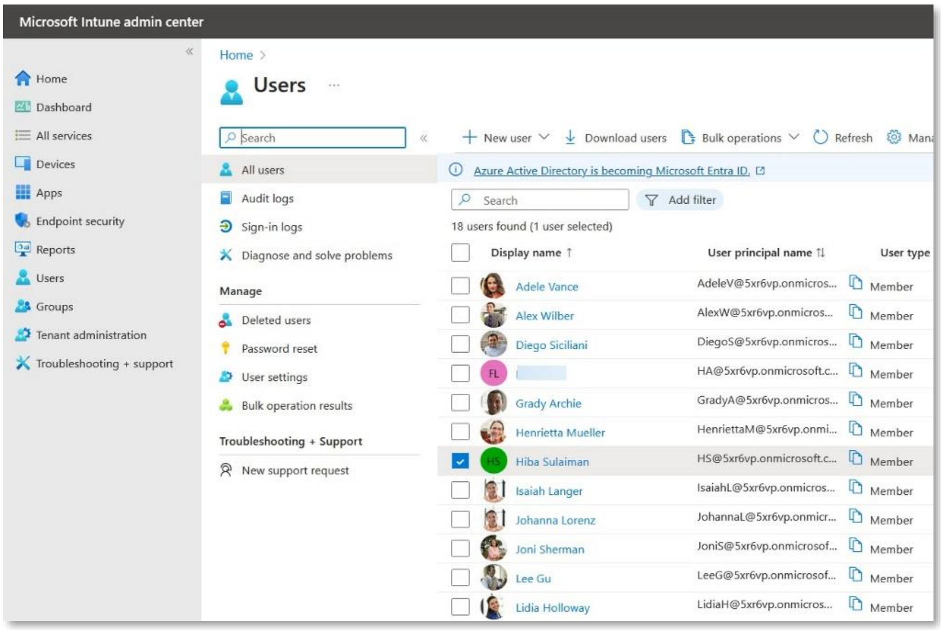
In Microsoft Intune, you can assign licenses to users or groups, so that they can enrol their devices. You can assign a license either to an individual user or to a group, so that the license is applied to all the users in a certain group.

Assign License to a User

Use the following steps to assign an Intune license to the added user:

1. Click Users from the left panel.

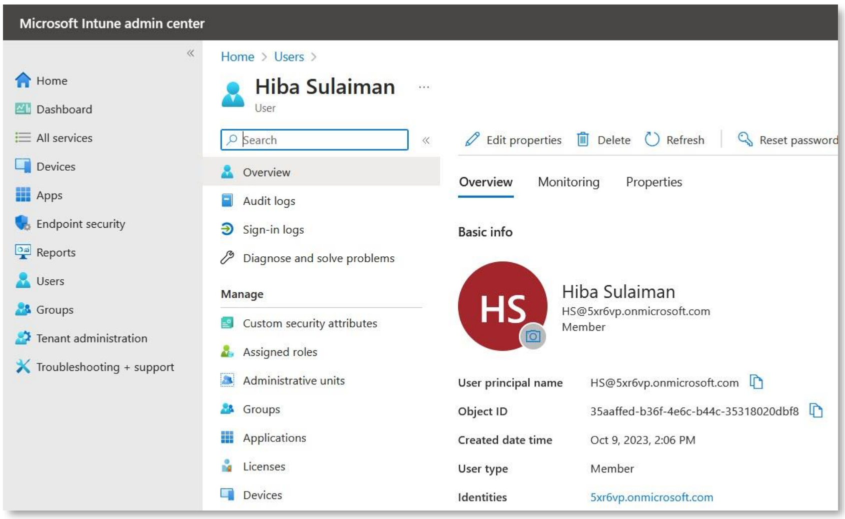
Then search and click on the user you added from the list, e.g. Hiba Sulaiman.



18 users found (1 user selected)

	Display name ↑	User principal name ↑↓	User type
□	Adele Vance	AdeleV@5xr6vp.onmicros...	Member
□	Alex Wilber	AlexW@5xr6vp.onmicros...	Member
□	Diego Siciliani	DiegoS@5xr6vp.onmicros...	Member
□	[redacted]	HA@5xr6vp.onmicrosoft.c...	Member
□	Grady Archie	GradyA@5xr6vp.onmicros...	Member
□	Henrietta Mueller	HenriettaM@5xr6vp.onmi...	Member
☑	Hiba Sulaiman	HS@5xr6vp.onmicrosoft.c...	Member
□	Isaiah Langer	IsaiahL@5xr6vp.onmicros...	Member
□	Johanna Lorenz	JohannaL@5xr6vp.onmicr...	Member
□	Joni Sherman	JoniS@5xr6vp.onmicrosof...	Member
□	Lee Gu	LeeG@5xr6vp.onmicrosof...	Member
□	Lidia Holloway	LidiaH@5xr6vp.onmicros...	Member

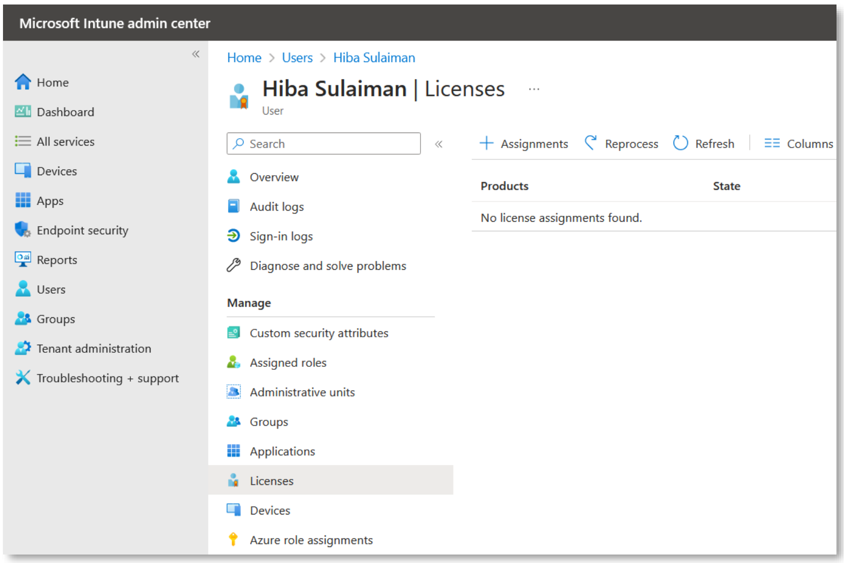
2. The Overview screen will be displayed. From the Manage tab, click Licenses.



Hiba Sulaiman
HS@5xr6vp.onmicrosoft.com
Member

User principal name	HS@5xr6vp.onmicrosoft.com
Object ID	35aaffed-b36f-4e6c-b44c-35318020dbf8
Created date time	Oct 9, 2023, 2:06 PM
User type	Member
Identities	5xr6vp.onmicrosoft.com

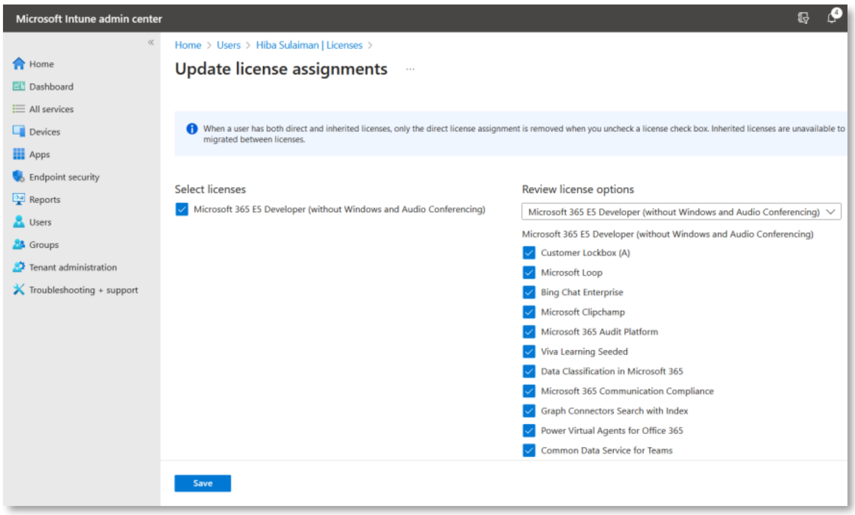
3. On the Licenses screen, click Assignments



No license assignments found.

4. Update license assignments screen will appear.

   Select licenses against the Microsoft 365 plan. Then select Microsoft 365 from the drop down, check all options and click Save.


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Users > Hiba Sulaiman | Licenses >
Update license assignments
Save

When a user has both direct and inherited licenses, only the direct license assignment is removed when you uncheck a license check box. Inherited licenses are unavailable to migrated between licenses.

Select licenses

☑ Microsoft 365 E5 Developer (without Windows and Audio Conferencing)

Review license options

Microsoft 365 E5 Developer (without Windows and Audio Conferencing)

Microsoft 365 E5 Developer (without Windows and Audio Conferencing)

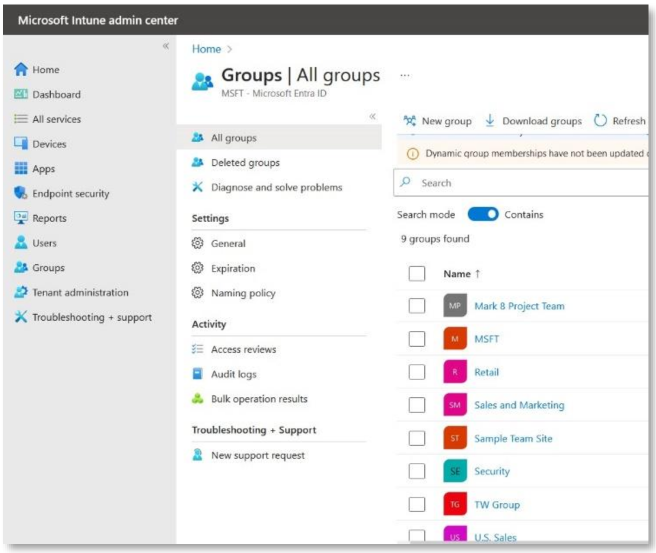
☑ Customer Lockbox (A)
☑ Microsoft Loop
☑ Bing Chat Enterprise
☑ Microsoft Clipchamp
☑ Microsoft 365 Audit Platform
☑ Viva Learning Seeded
☑ Data Classification in Microsoft 365
☑ Microsoft 365 Communication Compliance
☑ Graph Connectors Search with Index
☑ Power Virtual Agents for Office 365
☑ Common Data Service for Teams

Assign License to a Group

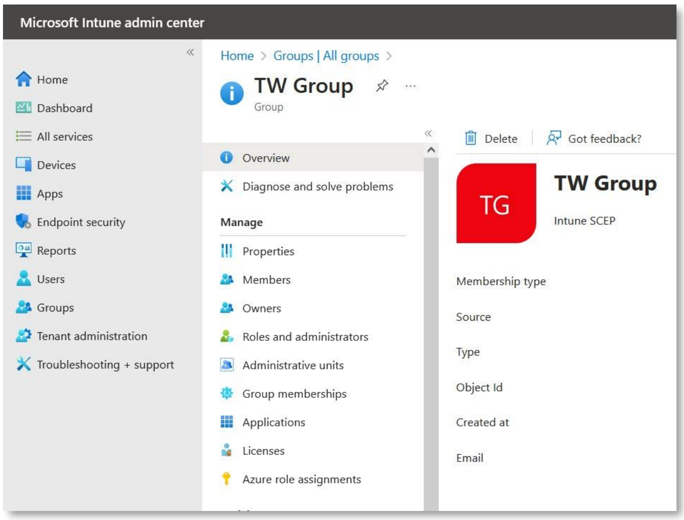
Use the following steps to assign an Intune license to the added group:

1. Click Groups**.**

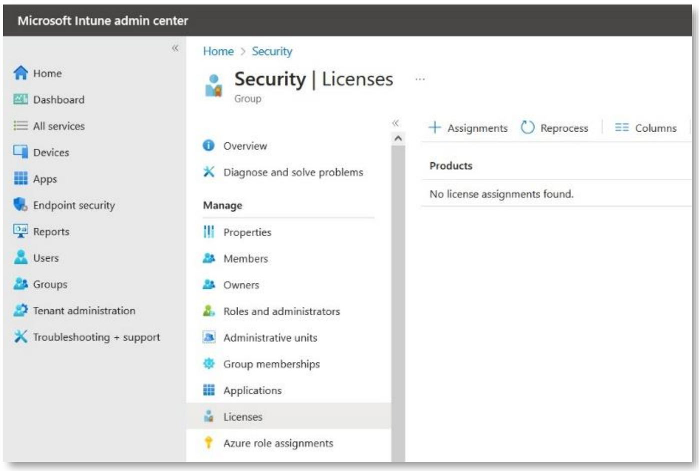
Select the added group e.g. TW Group.



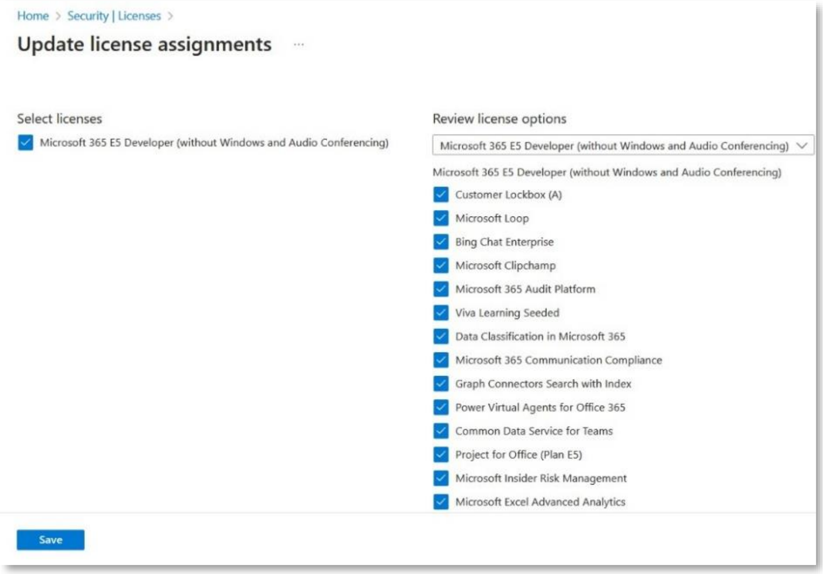
2. The Overview screen will be displayed. From the Manage tab, click Licenses.



3. On the Licenses screen, click Assignments.



4. Update license assignments screen will appear.
Select licenses against the Microsoft 365 plan.
Then select Microsoft 365 from the drop down, check all options and click Save.



Home > Security | Licenses >

Update license assignments ···

Select licenses

☑ Microsoft 365 E5 Developer (without Windows and Audio Conferencing)

Review license options

Microsoft 365 E5 Developer (without Windows and Audio Conferencing) ∨

Microsoft 365 E5 Developer (without Windows and Audio Conferencing)

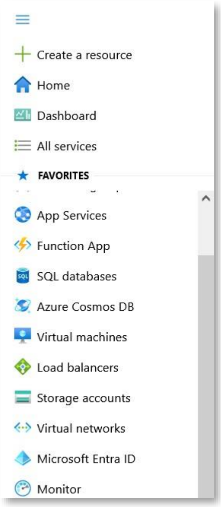
☑ Customer Lockbox (A)
☑ Microsoft Loop
☑ Bing Chat Enterprise
☑ Microsoft Clipchamp
☑ Microsoft 365 Audit Platform
☑ Viva Learning Seeded
☑ Data Classification in Microsoft 365
☑ Microsoft 365 Communication Compliance
☑ Graph Connectors Search with Index
☑ Power Virtual Agents for Office 365
☑ Common Data Service for Teams
☑ Project for Office (Plan E5)
☑ Microsoft Insider Risk Management
☑ Microsoft Excel Advanced Analytics

6.2. Authorize communication between CA and Intune

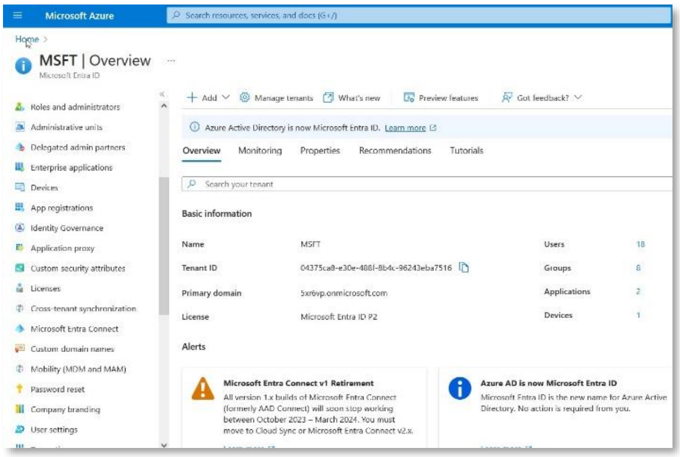
6.2.1. Add Mobile Device Management (MDM) Authority

A user needs to register the Mobile Device Management (MDM) authority to use Microsoft Intune. Access Azure portal https://portal.azure.com by using the credentials used in section 5.1.5.

1. From the Microsoft Azure portal home page, open the left menu, scroll and click on Microsoft Entra ID.



2. From the left menu under Manage, click Mobility (MDM and MAM).



Azure Active Directory is now Microsoft Entra ID. Learn more

Basic information

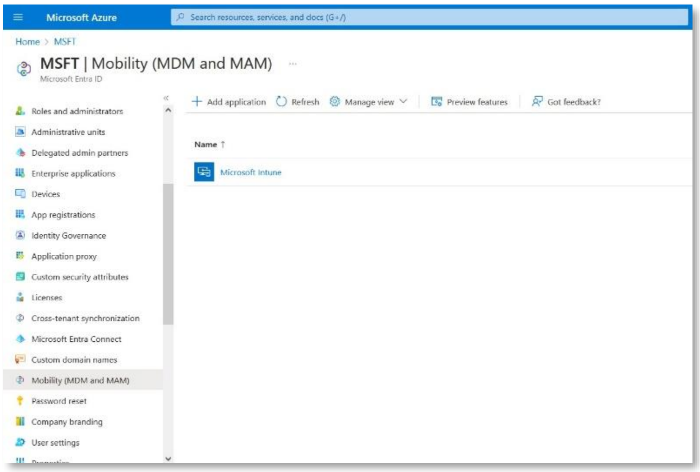
Name	MSFT	Users	18
Tenant ID	04375ca8-e30e-488l-8b4c-96243eba7516	Groups	8
Primary domain	5xr6vp.onmicrosoft.com	Applications	2
License	Microsoft Entra ID P2	Devices	1

Alerts

Microsoft Entra Connect v1 Retirement
All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.

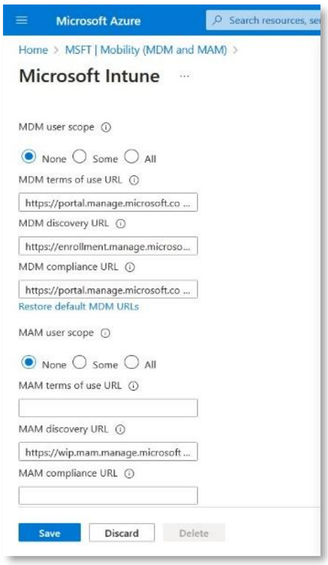
Azure AD is now Microsoft Entra ID
Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.

3. Then click Microsoft Intune.



Name ↑
Microsoft Intune

4. You can specify settings to allow All users to enrol a device, or choose to allow Some users (and specify a group).



Microsoft Intune

MDM user scope ● None ○ Some ○ All

MDM terms of use URL: https://portal.manage.microsoft.co ...

MDM discovery URL: https://enrollment.manage.microso...

MDM compliance URL: https://portal.manage.microsoft.co ...

Restore default MDM URLs

MAM user scope ● None ○ Some ○ All

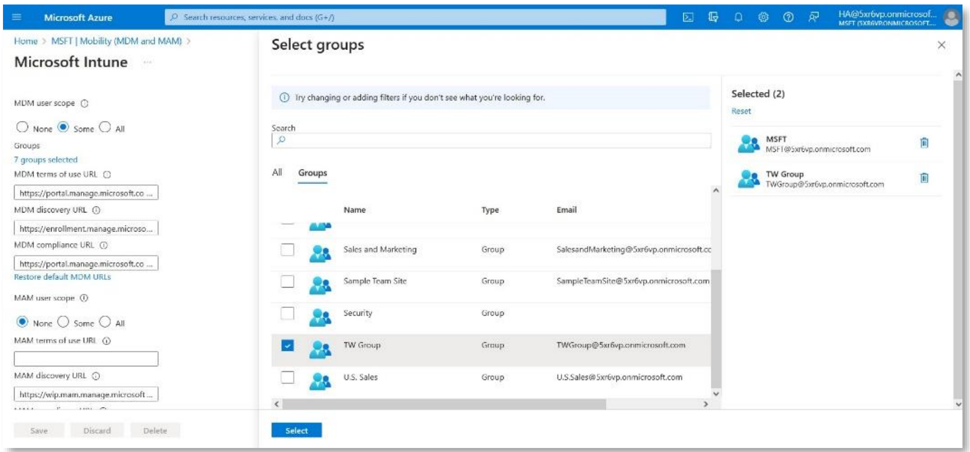
MAM terms of use URL:

MAM discovery URL: https://wip.mam.manage.microsoft ...

MAM compliance URL:

5. In this document we have selected Some.

Add group Select the group e.g. TW Group from the list and click Select.


Microsoft Azure
Search resources, services, and docs (G+/)
HA@5xr6vp.onmicrosof...
MSFT (5XR6VP.ONMICROSOFT...
Home > MSFT | Mobility (MDM and MAM) >
Save
Discard
Delete
Select

Microsoft Intune

MDM user scope ○ None ● Some ○ All

Groups: 7 groups selected

MDM terms of use URL: https://portal.manage.microsoft.co ...

MDM discovery URL: https://enrollment.manage.microso...

MDM compliance URL: https://portal.manage.microsoft.co ...

Restore default MDM URLs

MAM user scope ● None ○ Some ○ All

MAM terms of use URL:

MAM discovery URL: https://wip.mam.manage.microsoft ...

Select groups

Try changing or adding filters if you don't see what you're looking for.

Search

All | Groups

	Name	Type	Email
☐	Sales and Marketing	Group	SalesandMarketing@5xr6vp.onmicrosoft.cc
☐	Sample Team Site	Group	SampleTeamSite@5xr6vp.onmicrosoft.com
☐	Security	Group	
☑	TW Group	Group	TWGroup@5xr6vp.onmicrosoft.com
☐	U.S. Sales	Group	U.S.Sales@5xr6vp.onmicrosoft.com

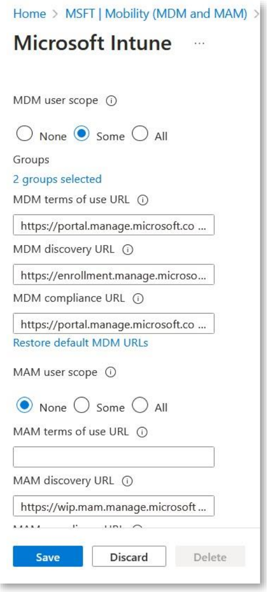
Selected (2)

Reset

MSFT MSFT@5xr6vp.onmicrosoft.com

TW Group TWGroup@5xr6vp.onmicrosoft.com

6. Then click Save.



Microsoft Intune

MDM user scope ○ None ● Some ○ All

Groups: 2 groups selected

MDM terms of use URL: https://portal.manage.microsoft.co ...

MDM discovery URL: https://enrollment.manage.microso...

MDM compliance URL: https://portal.manage.microsoft.co ...

Restore default MDM URLs

MAM user scope ● None ○ Some ○ All

MAM terms of use URL:

MAM discovery URL: https://wip.mam.manage.microsoft ...

6.3. Configure Intune Policy

After setting up both, Microsoft Intune and Microsoft Azure AD to activate Simple Certificate Enrolment Protocol (SCEP), you gain the ability to create SCEP profiles for users and devices. These profiles can be allocated within the Microsoft Intune environment.

However, for devices to utilize a SCEP certificate profile, it is essential to have a trusted root certificate. The establishment of trust for the root CA can be achieved through the deployment of a trusted certificate profile to the identical group that is granted the SCEP certificate profile.

Configure Intune Trusted Certificates and SCEP Certificate Profile

You need to create and configure the following Intune trusted certificates and SCEP certificate profile:

- Trusted Certificate profile for ADSS Web RA Root CA in Computer Certificate Store – Root.
- Trusted Certificate profile for ADSS Web RA Issuing CA in Computer Certificate Store – Intermediate.
- SCEP Certificate profile.

You are required to create and configure these three certificate profiles individually for each platform i.e. Android, iOS and Windows.

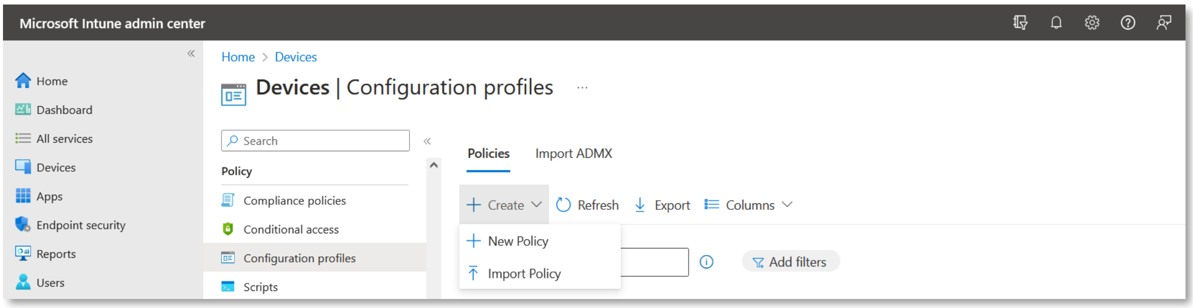
This document explains you to create and configure certificate profiles for Windows 10 or later. The steps for the other platforms i.e. Android and iOS will be the same.

6.3.1. Trusted Certificate Profile for ADSS Web RA Root CA

To create a Trusted Certificate profile for ADSS Web RA Root CA, follow the steps below:

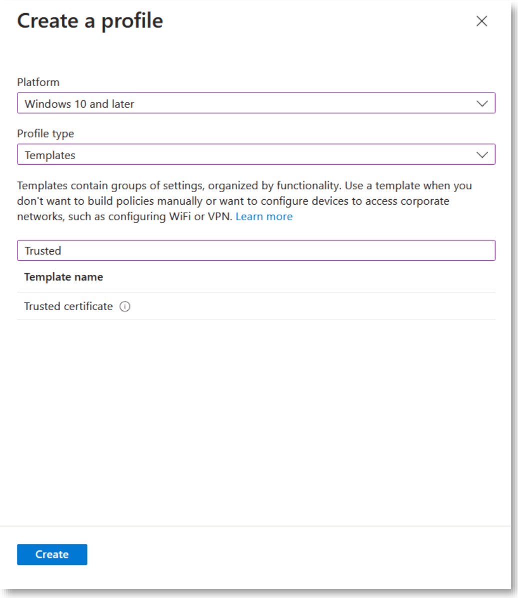
1. Go to the Microsoft Intune admin center, and click on Devices from the main left menu.

Under the Policy tab > Configuration profiles > Policies > Create > New Policy.



2. In the Create a profile tab, perform the following actions for Windows:

- Select the Platform as Windows 10 and later.
- Profile type as Templates,
- Search Trusted Certificate from the search bar in Template name and click Create.



Create a profile

Platform

Windows 10 and later

Profile type

Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

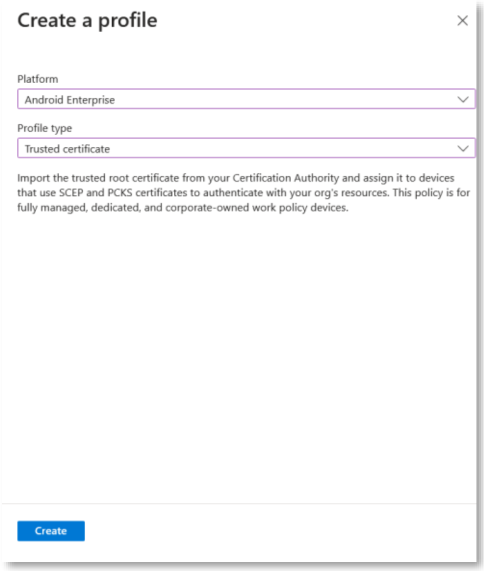
Trusted

Template name
Trusted certificate

If you are creating a profile for Android, perform the following actions at this step:

- Select the Platform as Android Enterprise.
- Profile type as Trusted certificate,

Then click Create.



Create a profile

Platform

Android Enterprise

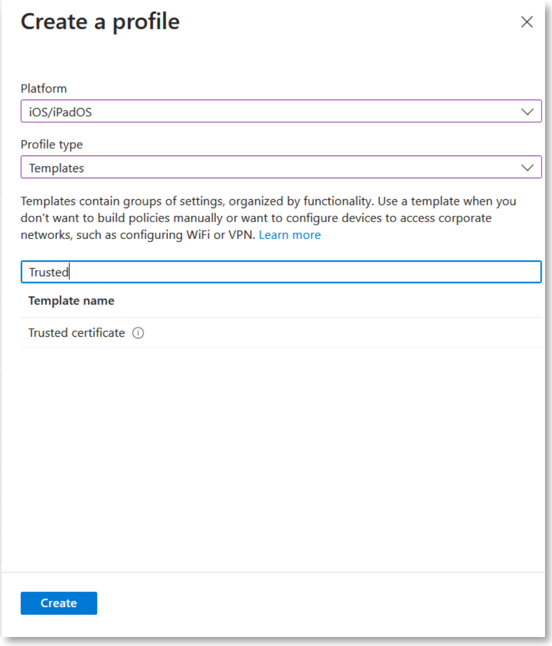
Profile type

Trusted certificate

Import the trusted root certificate from your Certification Authority and assign it to devices that use SCEP and PCKS certificates to authenticate with your org's resources. This policy is for fully managed, dedicated, and corporate-owned work policy devices.

If you are creating a profile for iOS, perform the following actions at this step:

- Select the Platform as iOS/iPadOS.
- Profile type as Templates. Once you select this option, the Trusted drop down will appear.



Create a profile

Platform: iOS/iPadOS

Profile type: Templates

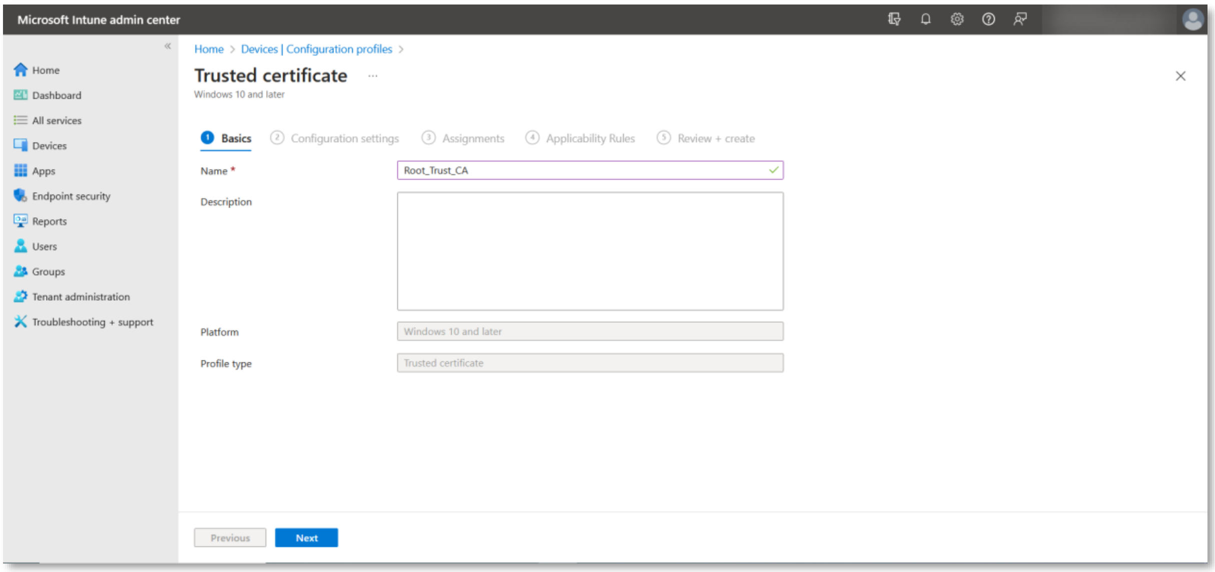
Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

Trusted

Template name
Trusted certificate ⓘ

3. In the Basics tab set:

A profile name for the Trusted Root Certificate. Then click Next.



Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Configuration profiles >

Trusted certificate

Windows 10 and later

Name *: Root_Trust_CA

Description:

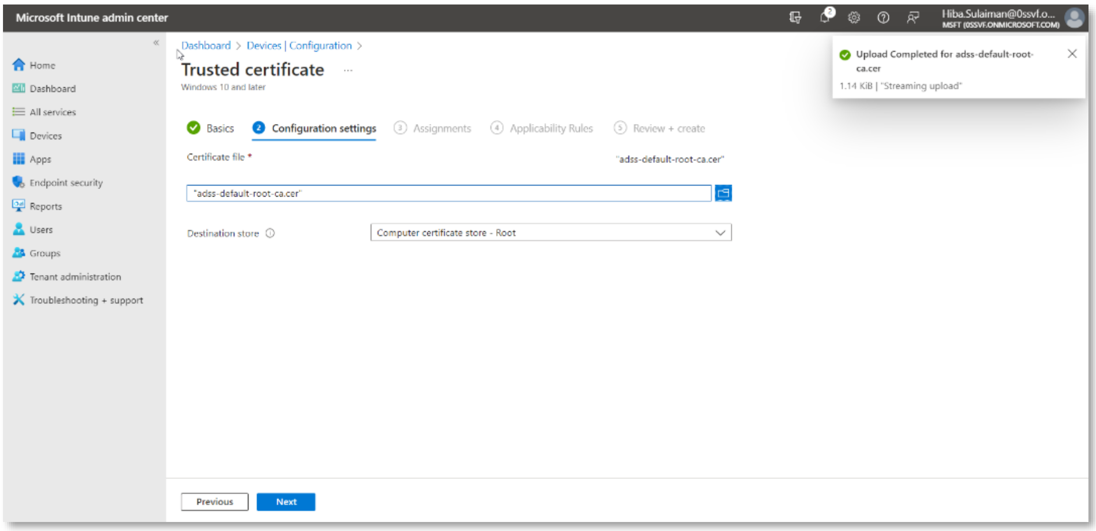
Platform: Windows 10 and later

Profile type: Trusted certificate

4. In the Configuration Settings tab perform the following actions:

Upload the Root CA Certificate – Here you can either:

- ○ Download the chain of certificates from ADSS Web RA mentioned in section 5.1.10 under the Enrolment Protocol (s) heading.
- ○ You can create your own Trusted chain from ADSS Server as mentioned in section 3.1.
- ○ If you have an existing CA certificate, you can use it here.
- Then from Destination store select Computer certificate store - Root, and then click Next.



Trusted certificate

Windows 10 and later

Upload Completed for adss-default-root-ca.cer

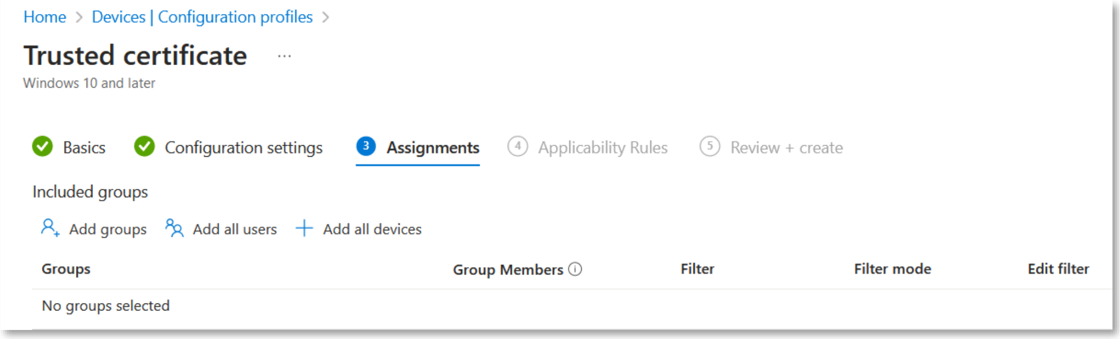
1.14 KiB | "Streaming upload"

Certificate file * "adss-default-root-ca.cer"

"adss-default-root-ca.cer"

Destination store: Computer certificate store - Root

5. In the Assignments tab, under Included groups, click Add groups.



Trusted certificate

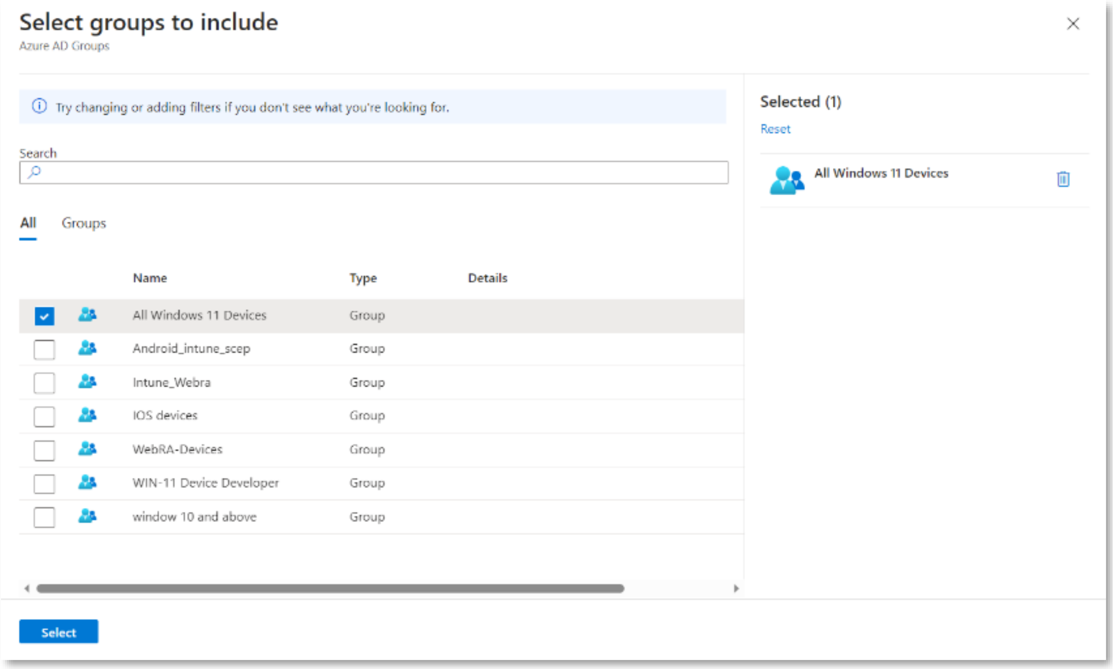
Windows 10 and later

Included groups

Groups	Group Members	Filter	Filter mode	Edit filter
No groups selected				

6. From Select groups to include:

Search and select your group e.g. All Windows 11 Devices it, and then click Select.



Select groups to include

Azure AD Groups

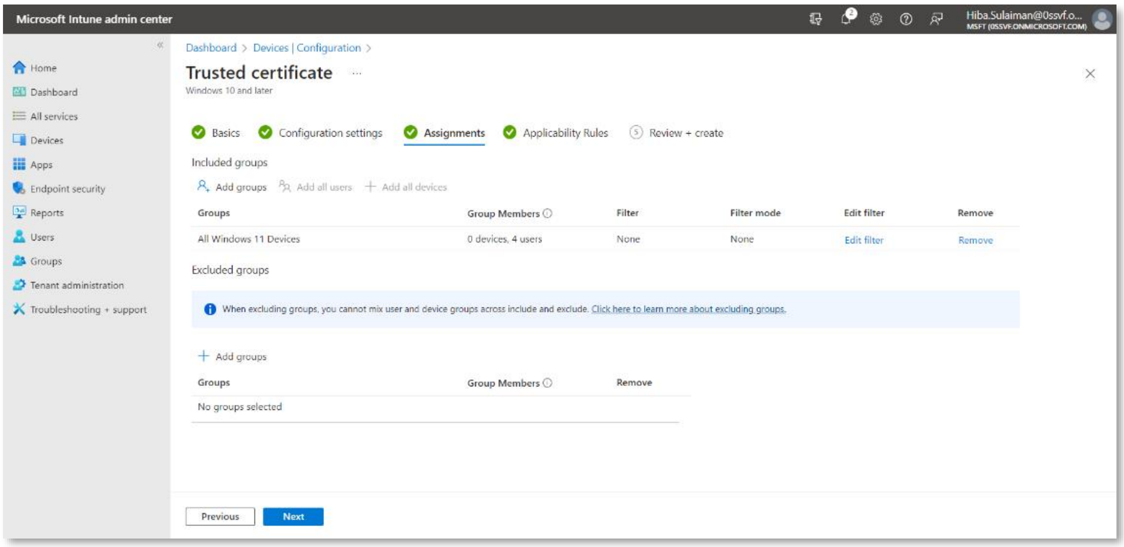
Try changing or adding filters if you don't see what you're looking for.

	Name	Type	Details
☑	All Windows 11 Devices	Group	
☐	Android_intune_scep	Group	
☐	Intune_Webra	Group	
☐	IOS devices	Group	
☐	WebRA-Devices	Group	
☐	WIN-11 Device Developer	Group	
☐	window 10 and above	Group	

Selected (1)

All Windows 11 Devices

7. The group will appear in the list of included groups, click Next. You can set the Applicability Rules, or leave the fields blank and then click Next to proceed.



Trusted certificate

Windows 10 and later

Included groups

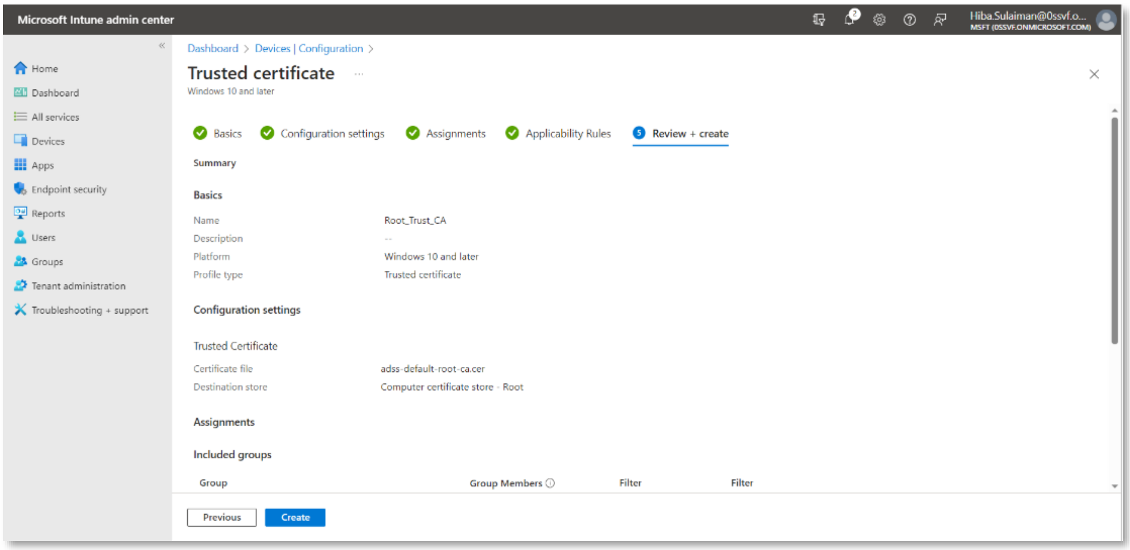
Groups	Group Members	Filter	Filter mode	Edit filter	Remove
All Windows 11 Devices	0 devices, 4 users	None	None	Edit filter	Remove

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Groups	Group Members	Remove
No groups selected		

8. On the Review + create tab, click Create.



Trusted certificate

Windows 10 and later

Summary

Basics

Name	Root_Trust_CA
Description	--
Platform	Windows 10 and later
Profile type	Trusted certificate

Configuration settings

Trusted Certificate

Certificate file	adss-default-root-ca.cer
Destination store	Computer certificate store - Root

Assignments

Included groups

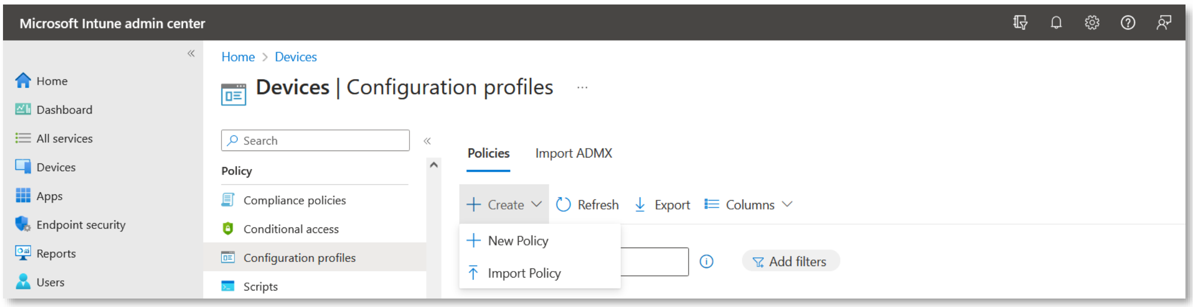
Group	Group Members	Filter	Filter

A certificate profile will appear in the listing. If it does not appear in the listing, click on the Refresh button.

6.3.2. Trusted Certificate Profile for ADSS Web RA Issuing CA

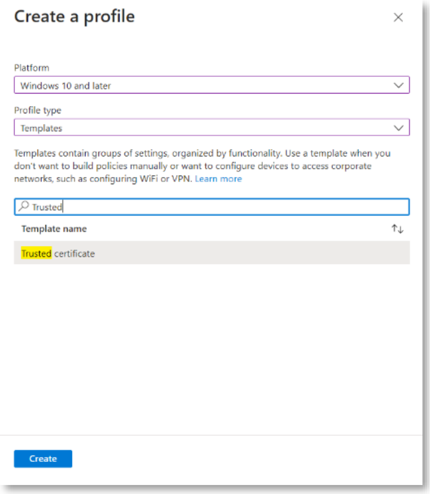
To create a Trusted Certificate profile for ADSS Web RA Issuing CA, follow the steps below:

1. Go to the Microsoft Intune admin center, and click on Devices from the main left menu. Under the Manage tab > Configuration profiles > Policies > Create > New Policy.



2. In the Create a profile tab:

- Select the Platform as Windows 10 and later,
- Profile type as Templates
- Search Trusted Certificate from the search bar in Template name and click Create.



Platform: Windows 10 and later

Profile type: Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

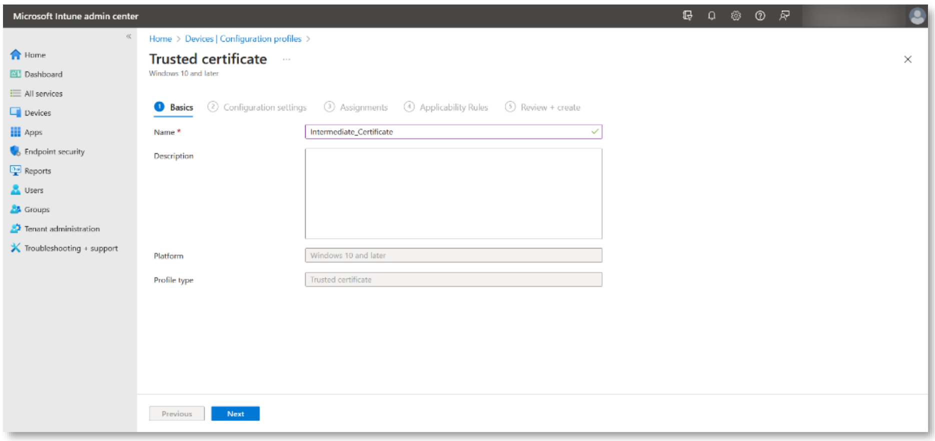
Trusted

Trusted certificate

3. In the Basics tab:

- Set a profile name for the Intermediate Certificate e.g. Intermediate_Certificate.

Then click Next.



Name *: Intermediate_Certificate

Description:

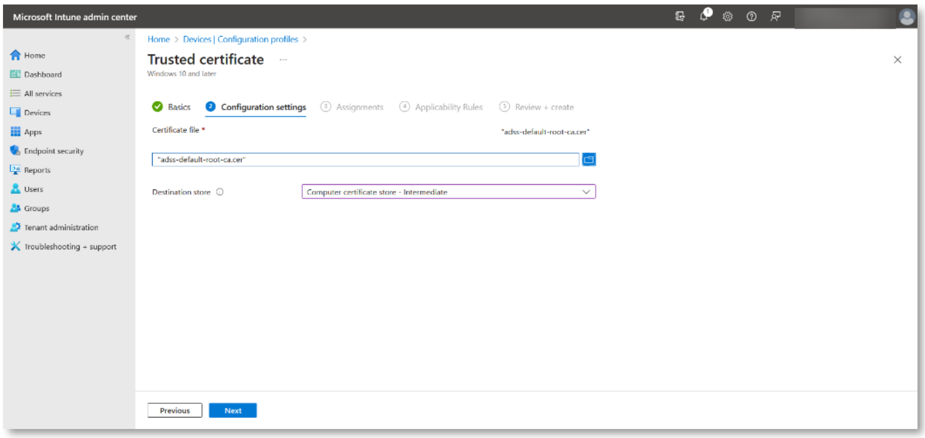
Platform: Windows 10 and later

Profile type: Trusted certificate

4. In the Configuration Settings tab,

Upload the Intermediate Certificate – Here you can either:

- ○ Download the chain of certificates from ADSS Web RA mentioned in section 5.1.10 under the Enrolment Protocol (s) heading.
- ○ You can create your own Trusted chain from ADSS Server as mentioned in section 3.1.
- ○ If you have an existing CA certificate, you can use it here.
- Then from Destination store select Intermediate certificate store - Root, and then click Next.



Home > Devices | Configuration profiles >

Trusted certificate

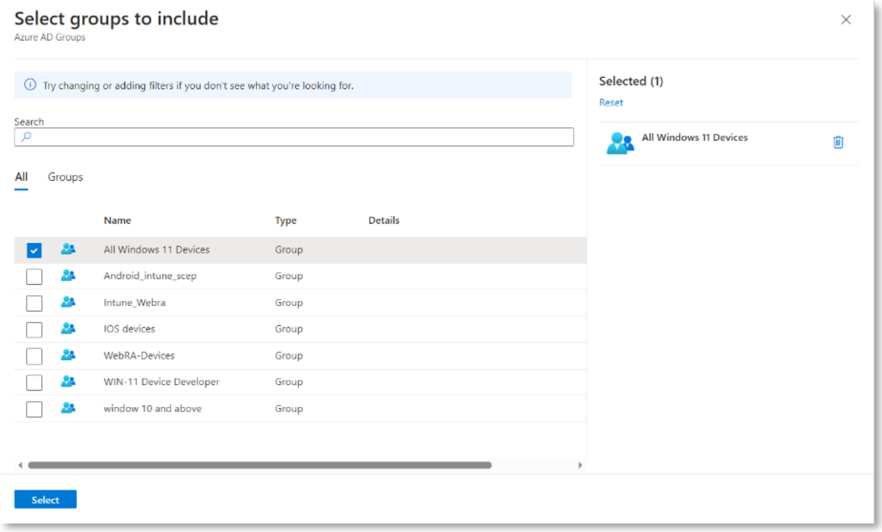
Windows 10 and later

Certificate file *: "adss-default-root-ca.cer"

Destination store: Computer certificate store - Intermediate

5. In the Assignments tab:

- From the Included groups click Add group.
- Then select the groups to include, e.g. All Windows 11 Devices, and click Select.



Select groups to include

Azure AD Groups

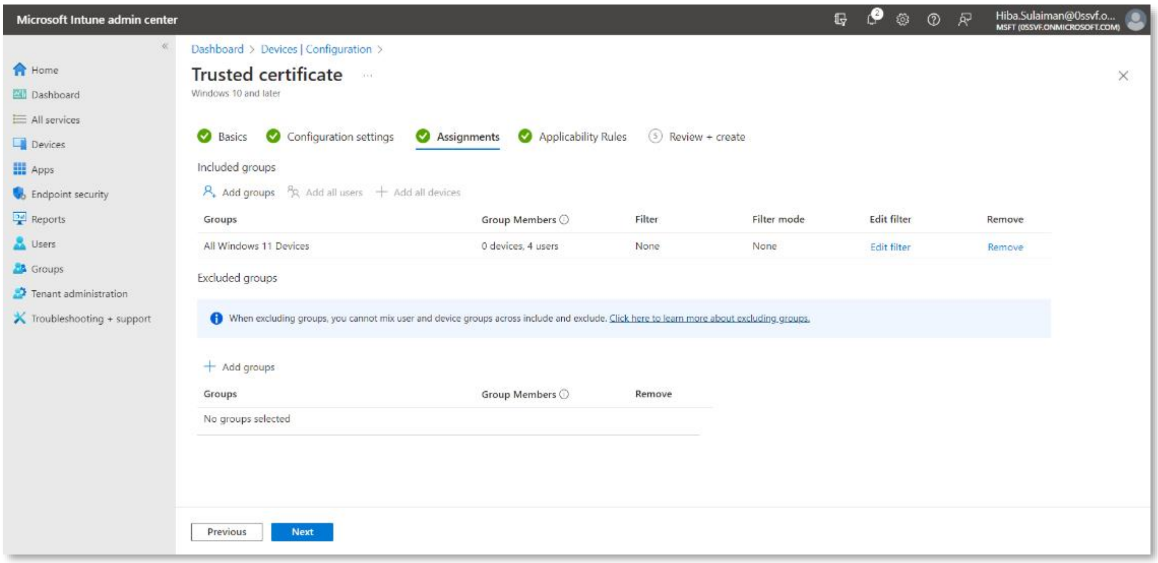
Try changing or adding filters if you don't see what you're looking for.

		Name	Type	Details
☑		All Windows 11 Devices	Group	
□		Android_intune_scep	Group	
□		Intune_Webra	Group	
□		IOS devices	Group	
□		WebRA-Devices	Group	
□		WIN-11 Device Developer	Group	
□		window 10 and above	Group	

Selected (1)

All Windows 11 Devices

6. The group will appear in the list of included groups, click Next. You can set the Applicability Rules, or leave the fields blank and then click Next to proceed.



Trusted certificate

Windows 10 and later

Included groups

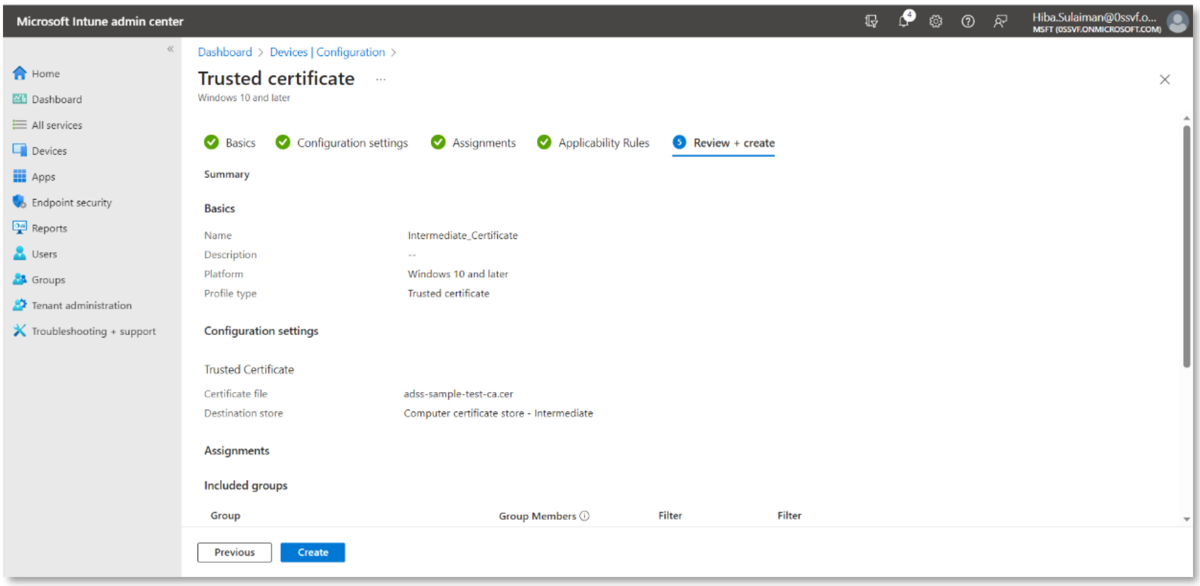
Groups	Group Members	Filter	Filter mode	Edit filter	Remove
All Windows 11 Devices	0 devices, 4 users	None	None	Edit filter	Remove

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Groups	Group Members	Remove
No groups selected		

7. On the Review + create tab, click Create.



Trusted certificate

Windows 10 and later

Summary

Basics

Name	Intermediate_Certificate
Description	--
Platform	Windows 10 and later
Profile type	Trusted certificate

Configuration settings

Trusted Certificate

Certificate file	adss-sample-test-ca.cer
Destination store	Computer certificate store - Intermediate

Assignments

Included groups

Group	Group Members	Filter	Filter

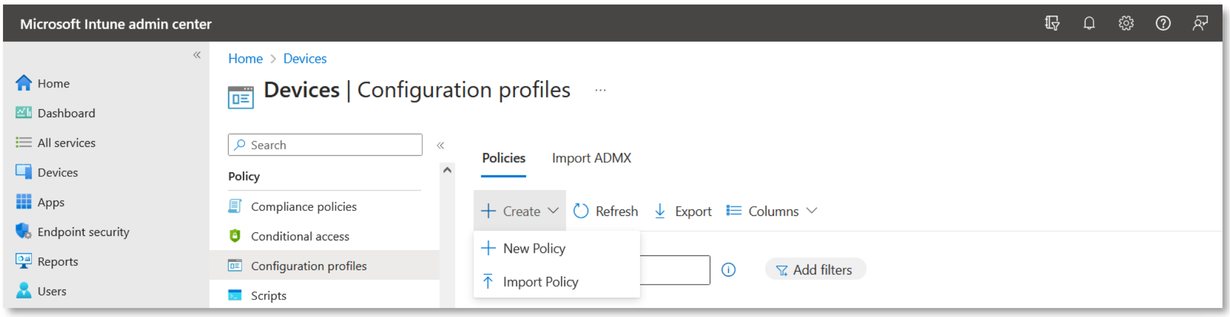
A certificate profile will appear in the listing. If it does not appear in the listing, click on the Refresh button.

6.3.3. SCEP Configuration Profile

To create a SCEP Configuration profile, follow the steps below:

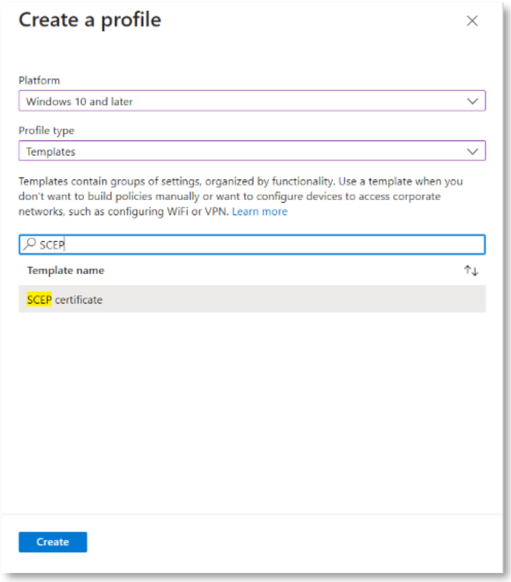
1. In the Microsoft Intune admin center, click on Devices from the main left menu.

Under the Policy tab, > Configuration > Policies > Create > New Policy.



2. In the Create a profile tab perform the following actions:

- Select the Platform as Windows 10 and later.
- Profile type as Templates.
- Search SCEP Certificate from the search bar in Template name and click Create.



Create a profile

Platform: Windows 10 and later

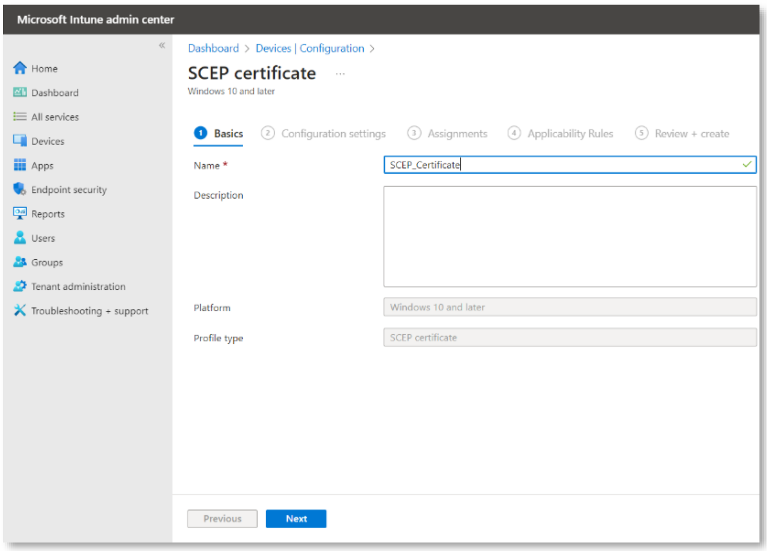
Profile type: Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

SCEP

Template name
SCEP certificate

3. In the Basics tab, set a profile name for the SCEP Certificate. Then click Next.



SCEP certificate

Windows 10 and later

Name *: SCEP_Certificate

Description:

Platform: Windows 10 and later

Profile type: SCEP certificate

4. While creating a SCEP certificate, in the Configuration settings tab, fill in the following fields:

Certificate type

Select a certificate type from the drop down.

- **User**

You can create two types of user certificates:

- User certificate
- User device certificate

- **Device**
  - Device certificate

Subject name format

The options for the subject name format depend on the certificate type you select, either user, or device. You can also create a user device certificate, which is explained below:

- **Subject name format if you are creating a user certificate:**

To create a user certificate, enter a custom subject name format, for common name and email. You can learn more about setting variables by clicking on the info button next to the subject name format.

CN={{UserName}} - The user name of the user.

E={{EmailAddress}} - The email address of the user.

- **Subject name format if you are creating a user device certificate:**

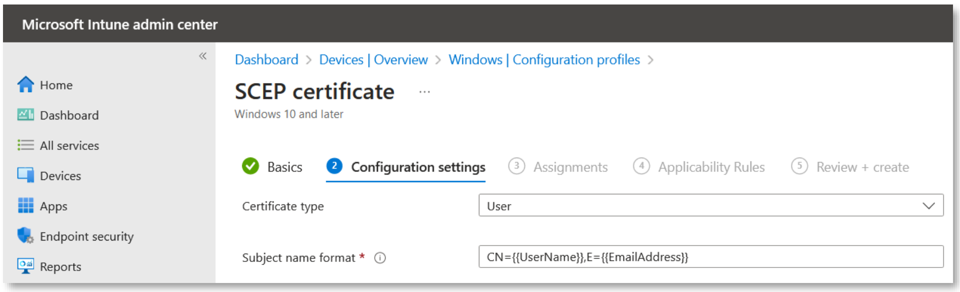
To create a user device certificate, enter a custom subject name format, for common name and email.
CN={{DeviceName}} - The name of the user device.
E={{EmailAddress}} - The email address of the user.

- Subject name format if you are creating a **device certificate:**

To create a device certificate, enter a custom subject name format, for common name. You can learn more about setting variables by clicking on the info button next to the subject name format.

CN={{AAD_Device_ID}} - This is used to identify a device by its Azure AD ID.

In this document, we are creating a user certificate.



SCEP certificate ...
Windows 10 and later

Certificate type: User

Subject name format *: CN={{UserName}},E={{EmailAddress}}

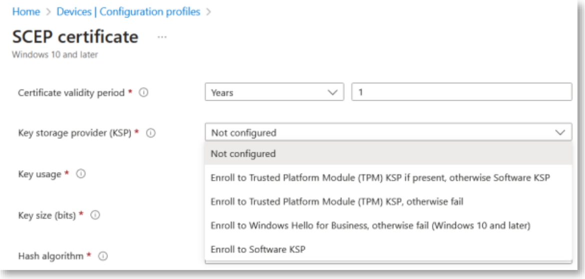
- Certificate validity period

You can select the duration in days, months or years, e.g. Years, 1.

- Key storage provider (KSP)

Specify where the key to the certificate is stored. Choose from the following values:

- Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP
- Enroll to Trusted Platform Module (TPM) KSP, otherwise fail
- Enroll to Windows Hello for Business, otherwise fail (Windows 10 and later)
- Enroll to Software KSP


Home > Devices | Configuration profiles >
Key usage *
Key size (bits) *
Hash algorithm *
Not configured
Not configured
Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP
Enroll to Trusted Platform Module (TPM) KSP, otherwise fail
Enroll to Windows Hello for Business, otherwise fail (Windows 10 and later)
Enroll to Software KSP

SCEP certificate ...
Windows 10 and later

Certificate validity period *: Years 1

Key storage provider (KSP) *: Not configured

- Key usage

Select either both or one of the two options, e.g. Digital signature and Key encipherment from this drop down.

- Key size

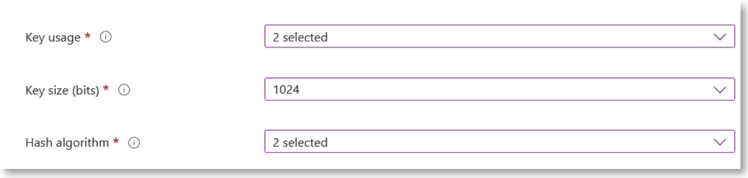
Select the number of bits contained in the key:

- ○ Not configured
- ○ 1024
- ○ 2048
- ○ 4096

- Hash Algorithm

Select one of the available hash algorithm types to use with this certificate.

- ○ SHA-1
- ○ SHA-2 or you may select both.



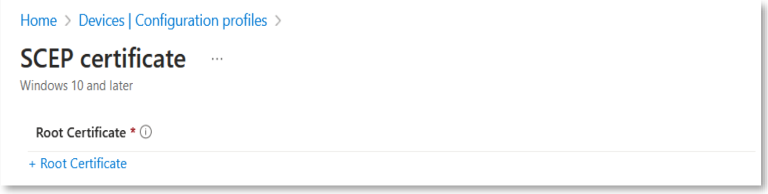
Key usage * : 2 selected

Key size (bits) * : 1024

Hash algorithm * : 2 selected

Scroll down to fill in the remaining fields.

- + Root Certificate



Home > Devices | Configuration profiles >

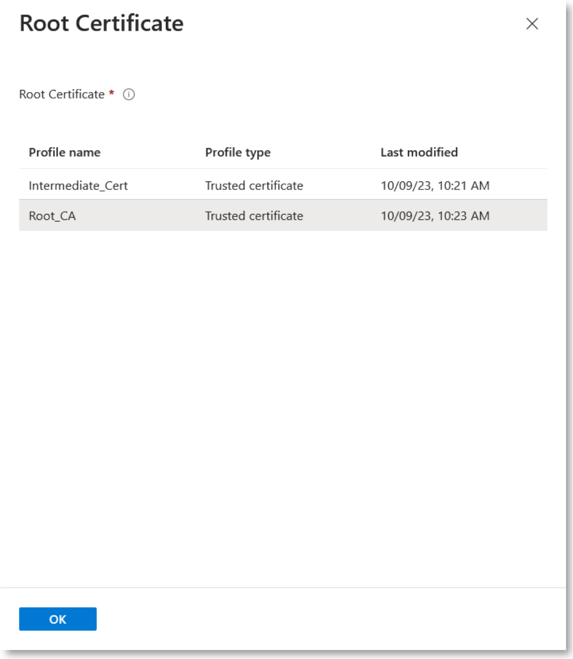
SCEP certificate ...

Windows 10 and later

Root Certificate *

+ Root Certificate

Select the trusted certificate you created in section 6.4.1 and click OK.



Root Certificate

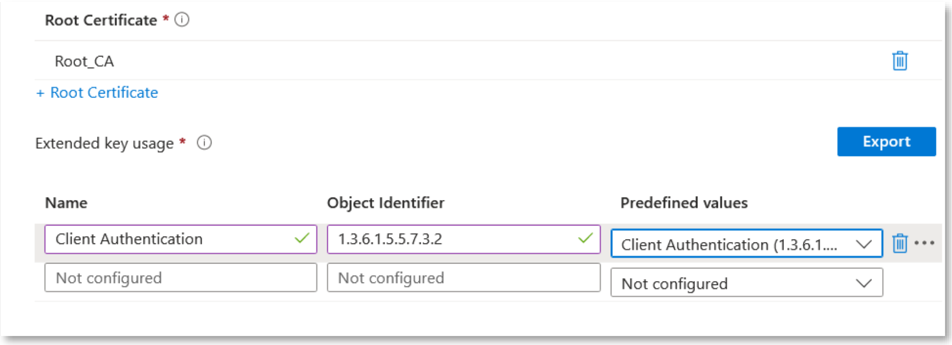
Root Certificate *

Profile name	Profile type	Last modified
Intermediate_Cert	Trusted certificate	10/09/23, 10:21 AM
Root_CA	Trusted certificate	10/09/23, 10:23 AM

The trusted root certificate will be uploaded.

- Extended key usage

Add values for the certificate's intended purpose. In most cases, the certificate requires client authentication so that the user or device can authenticate to a server. Once you select, the Object Identifier and Name will be auto-filled.



Root Certificate * ⓘ

Root_CA

Extended key usage * ⓘ

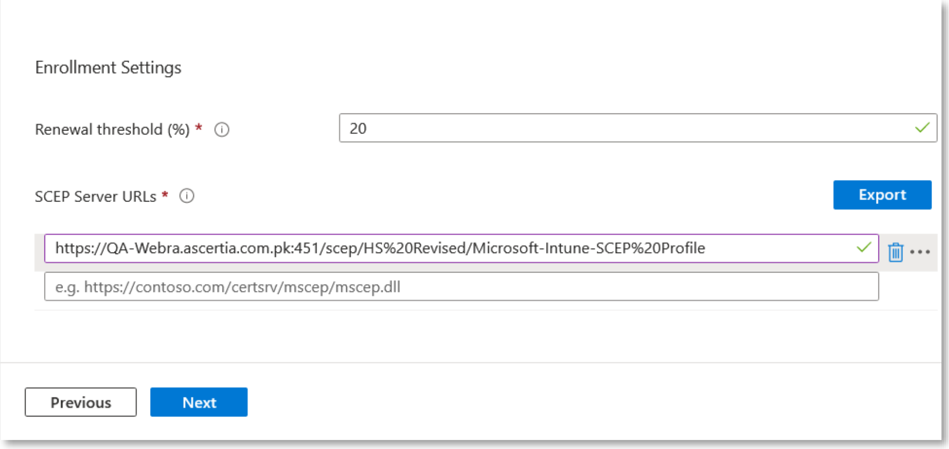
Name	Object Identifier	Predefined values
Client Authentication	1.3.6.1.5.5.7.3.2	Client Authentication (1.3.6.1....
Not configured	Not configured	Not configured

- Enrollment Settings

Renewal threshold (%) - Enter the percentage of the certificate lifetime that remains before the device requests renewal of the certificate. For example, if you enter 20, the renewal of the certificate will be attempted when the certificate is 80% expired.

- SCEP Server URLs

  At this step, copy the SCEP Profile URL that you created in Section 5.1.10 point number 12 and paste the URL here. Then click Next.



Enrollment Settings

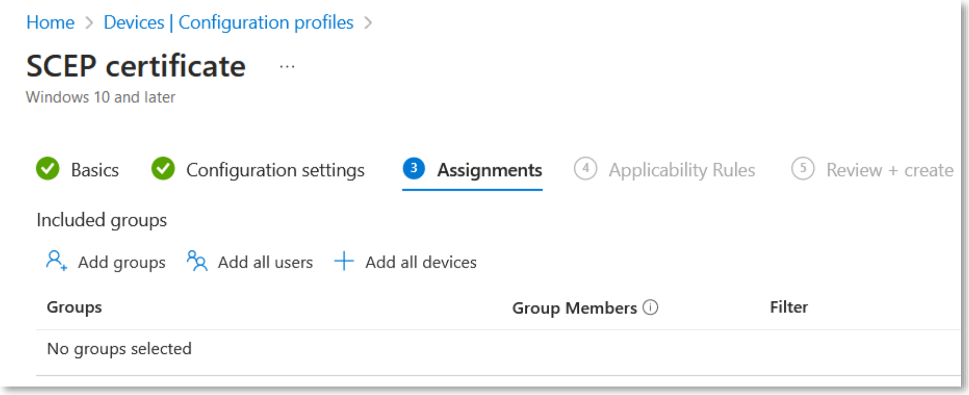
Renewal threshold (%) * ⓘ 20

SCEP Server URLs * ⓘ

https://QA-Webra.ascertia.com.pk:451/scep/HS%20Revised/Microsoft-Intune-SCEP%20Profile

e.g. https://contoso.com/certsrv/mscep/mscep.dll

5. In the Assignments tab, from the Included groups click Add groups.



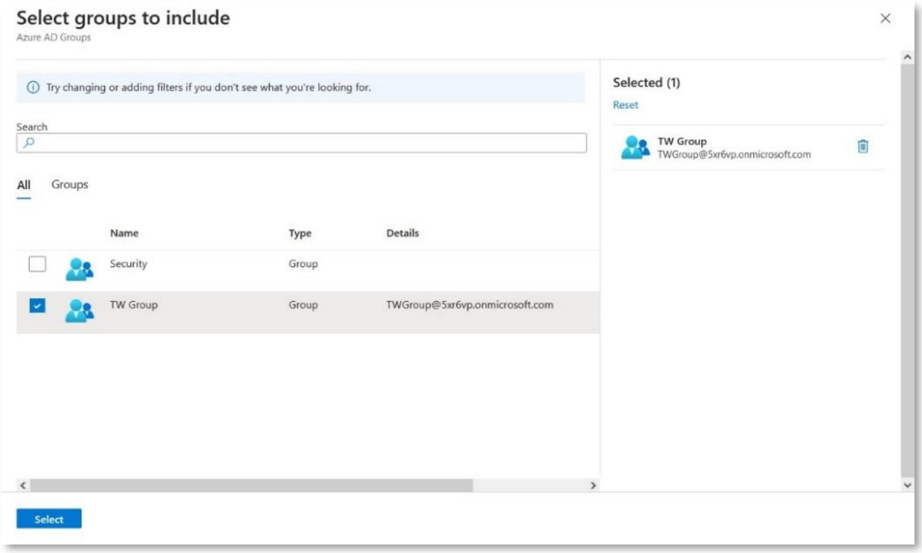
SCEP certificate

Windows 10 and later

Included groups

Groups	Group Members ⓘ	Filter
No groups selected		

6. Then select the groups to include and click Select.



Select groups to include

Azure AD Groups

Try changing or adding filters if you don't see what you're looking for.

Search

All Groups

	Name	Type	Details
□	Security	Group	
☑	TW Group	Group	TWGroup@5xr6vp.onmicrosoft.com

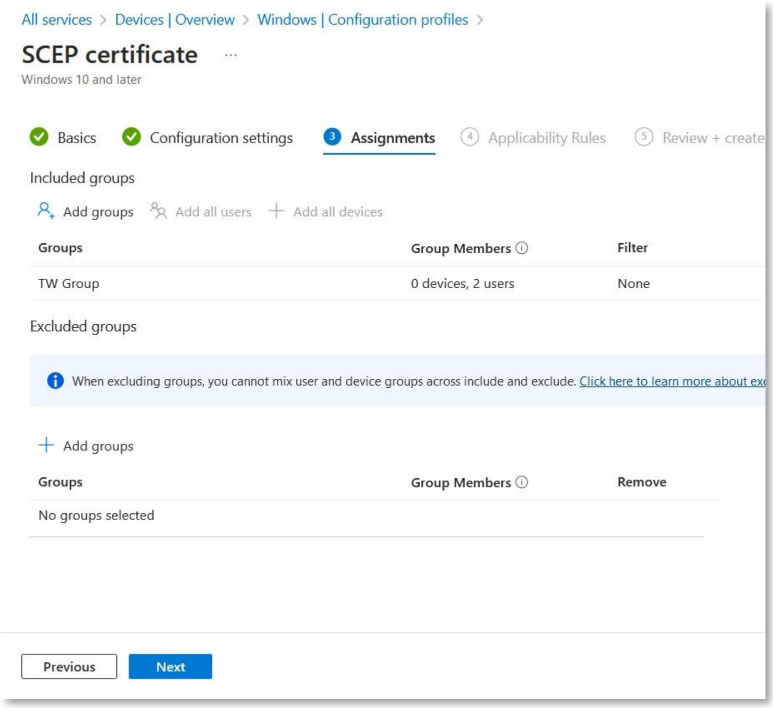
Selected (1)

Reset

TW Group
TWGroup@5xr6vp.onmicrosoft.com

Select

7. The group will appear in the list of included groups, click Next. You can set the Applicability Rules, or leave the fields blank and then click Next to proceed.



All services > Devices | Overview > Windows | Configuration profiles >

SCEP certificate

Windows 10 and later

Basics · Configuration settings · 3 Assignments · 4 Applicability Rules · 5 Review + create

Included groups

Add groups · Add all users · Add all devices

Groups	Group Members	Filter
TW Group	0 devices, 2 users	None

Excluded groups

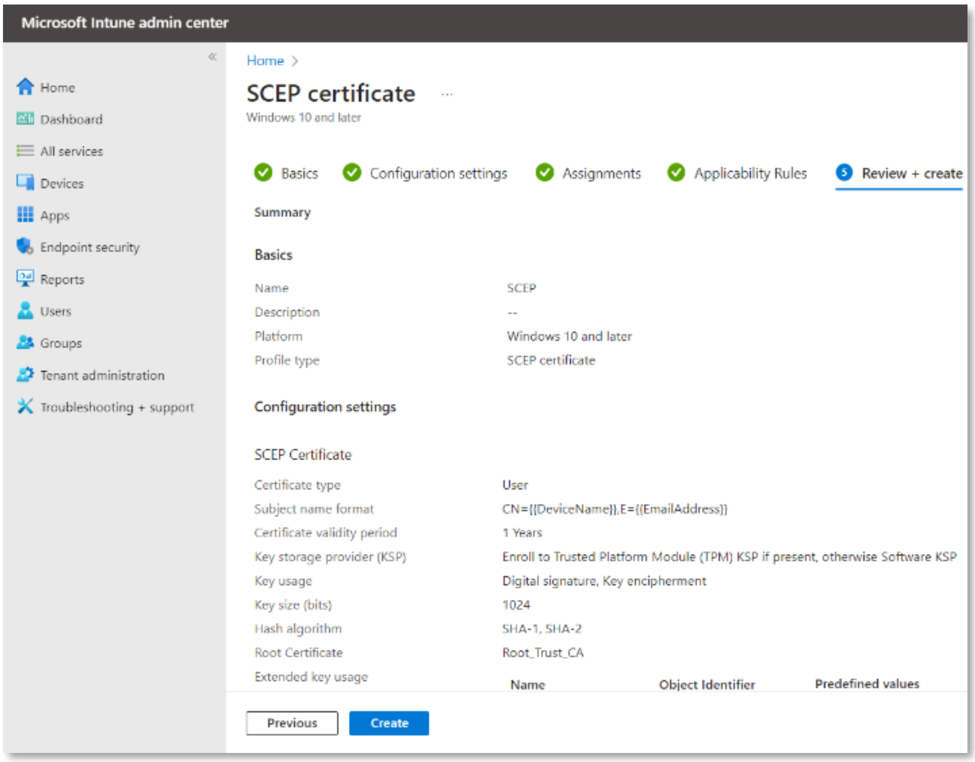
When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about exc

Add groups

Groups	Group Members	Remove
No groups selected		

Previous · Next

8. On the Review + create tab, click Create.



Summary

Basics

Name	SCEP
Description	--
Platform	Windows 10 and later
Profile type	SCEP certificate

Configuration settings

SCEP Certificate

Certificate type	User
Subject name format	CN={{DeviceName}},E={{EmailAddress}}
Certificate validity period	1 Years
Key storage provider (KSP)	Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP
Key usage	Digital signature, Key encipherment
Key size (bits)	1024
Hash algorithm	SHA-1, SHA-2
Root Certificate	Root_Trust_CA
Extended key usage	

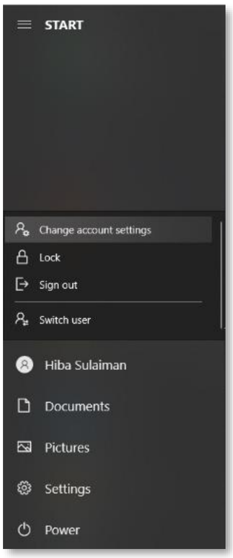
Name	Object Identifier	Predefined values

You have created a SCEP certificate profile successfully.

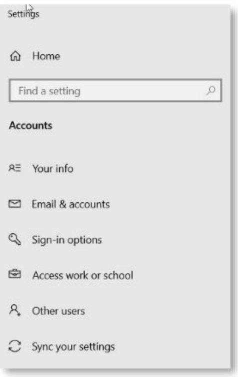
6.3.4. Windows Enrolment for Intune Policy

Log in to your Windows account with your Microsoft Intune user by following these steps:

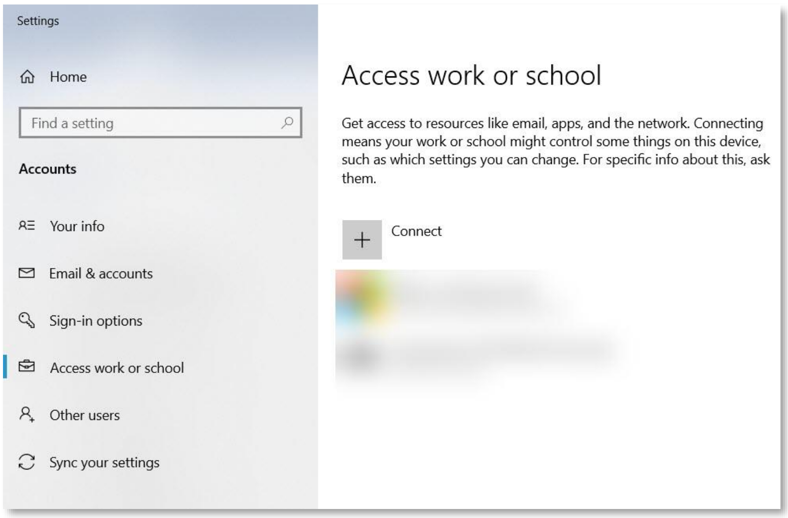
1. Log in to Windows account using your Microsoft Intune domain administrator, e.g. HA@5xr6vp.onmicrosoft.com.
2. From the Start button, launch Settings and scroll to your user e.g. Hiba Sulaiman > Change account settings.



3. Click Access work or school account.



4. Then click on Connect.

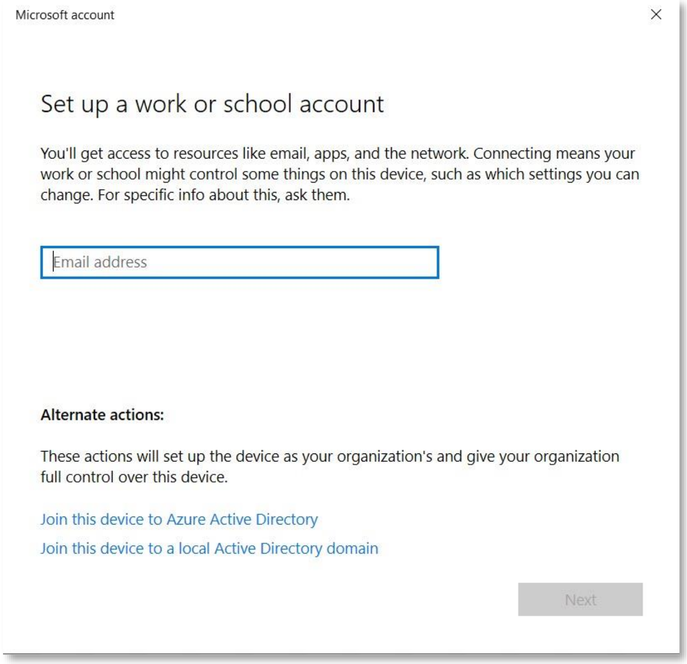


Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

5. From the alternate actions:

Click Join this device to Azure Active Directory.



Microsoft account

Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Email address

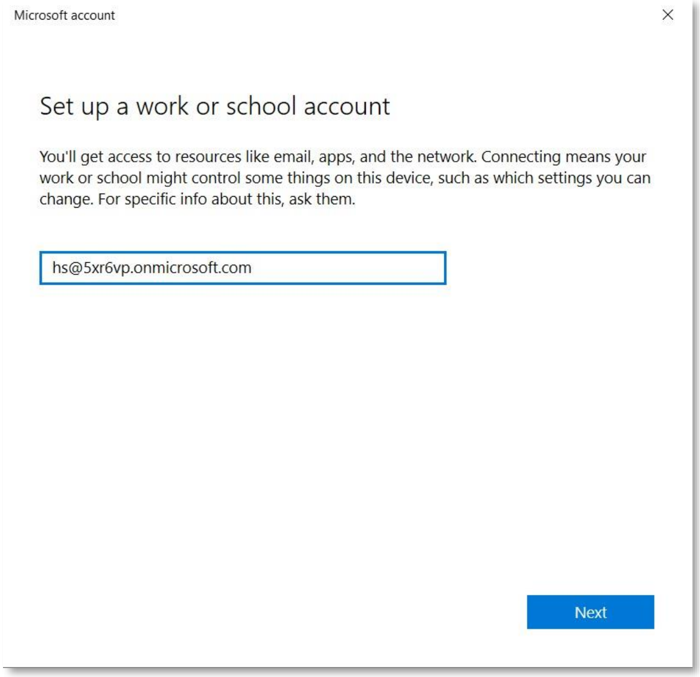
Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

Join this device to Azure Active Directory

Join this device to a local Active Directory domain

6. Enter your Microsoft Intune account e.g. HS@5xr6vp.onmicrosoft.com and click Next.



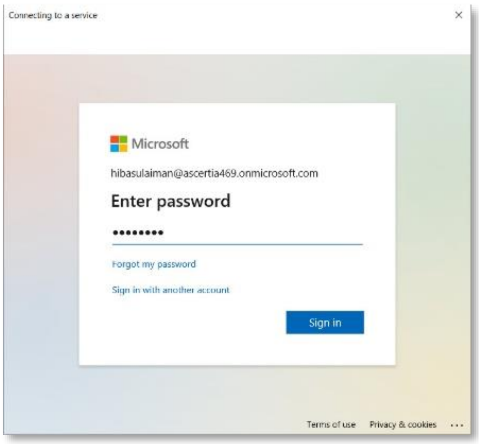
Microsoft account

Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

hs@5xr6vp.onmicrosoft.com

7. You will be required to enter your password, and then click Sign-in.

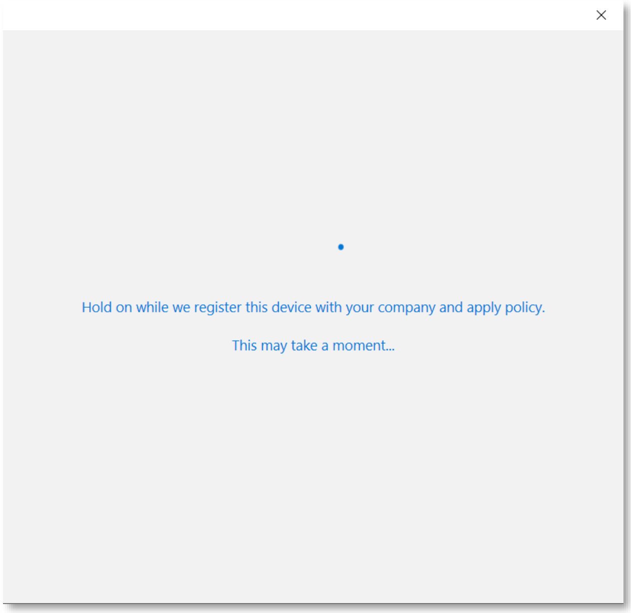


hibasulaiman@ascertia469.onmicrosoft.com

Enter password

••••••••

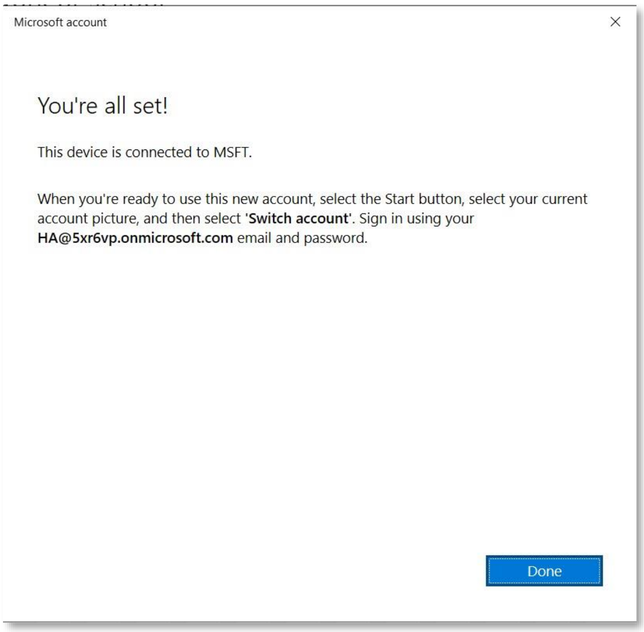
8. It may take some time to register the device with your company an apply policy.



Hold on while we register this device with your company and apply policy.

This may take a moment...

9. Success message appears. Click Done.



You're all set!

This device is connected to MSFT.

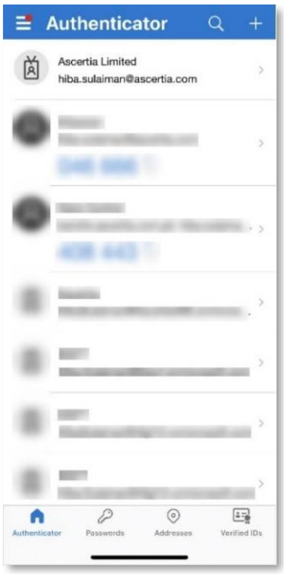
When you're ready to use this new account, select the Start button, select your current account picture, and then select '**Switch account**'. Sign in using your **HA@5xr6vp.onmicrosoft.com** email and password.

10. In the next step, you need to link your Windows account to Microsoft Authenticator app on your mobile device. Make sure you use your Microsoft Intune account credentials to log in to the Authenticator app.

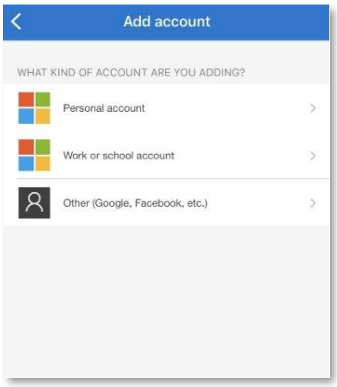
Microsoft Authenticator app

Follow the steps below to link your Microsoft Intune account with Microsoft Authenticator:

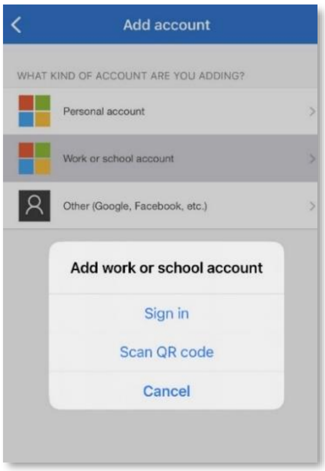
- Launch the Microsoft Authenticator app on your mobile device and tap +.



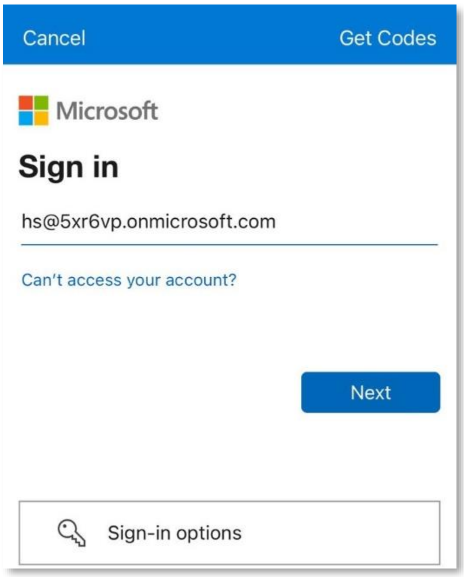
- On Add account, tap Add work or school account.


Add account
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)

- Choose an option to Sign-in


Add account
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)
Add work or school account
Sign in
Scan QR code
Cancel

- Enter your Microsoft Intune email address and tap Next.

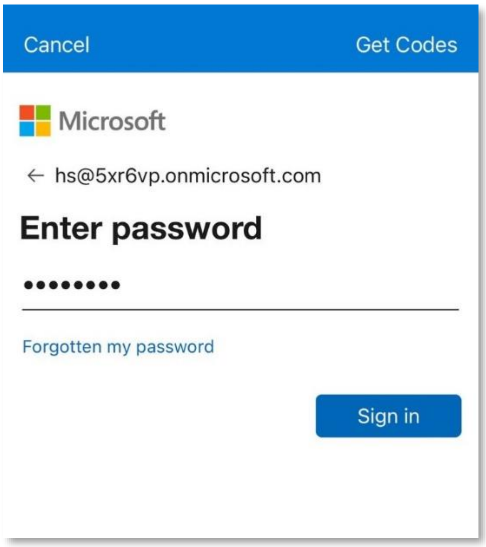


Sign in

hs@5xr6vp.onmicrosoft.com

Can't access your account?

- Enter your password and tap Sign in.



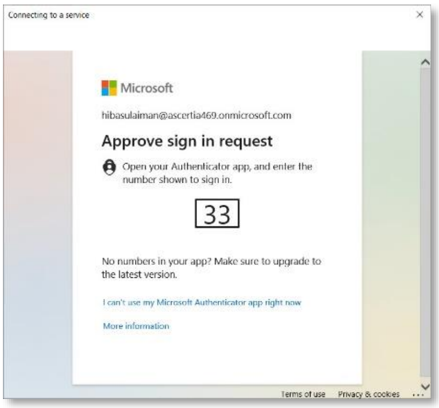
← hs@5xr6vp.onmicrosoft.com

Enter password

••••••••

Forgotten my password

- A code from Authenticator app will appear. Access your mobile phone to enter the code that appears on the screen.



hibasulaiman@ascertia469.onmicrosoft.com

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

33

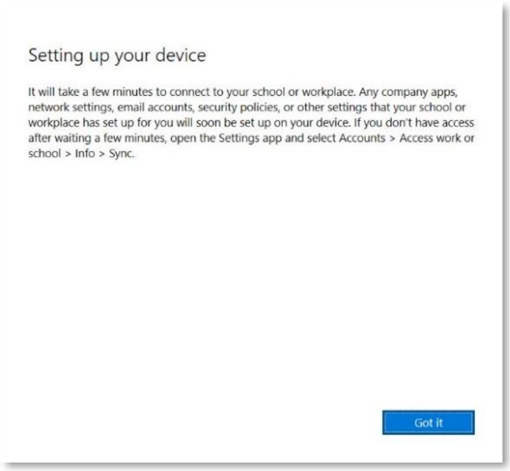
No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

More information

s

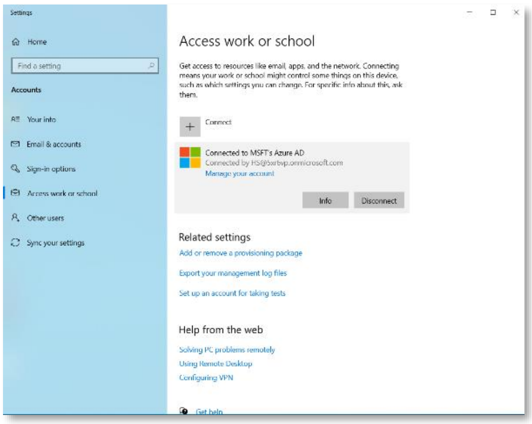
- Setting up your device confirmation will appear. Click Got it to complete the setup.



Setting up your device

It will take a few minutes to connect to your school or workplace. Any company apps, network settings, email accounts, security policies, or other settings that your school or workplace has set up for you will soon be set up on your device. If you don't have access after waiting a few minutes, open the Settings app and select Accounts > Access work or school > Info > Sync.

11. Your account will be added, click Info.



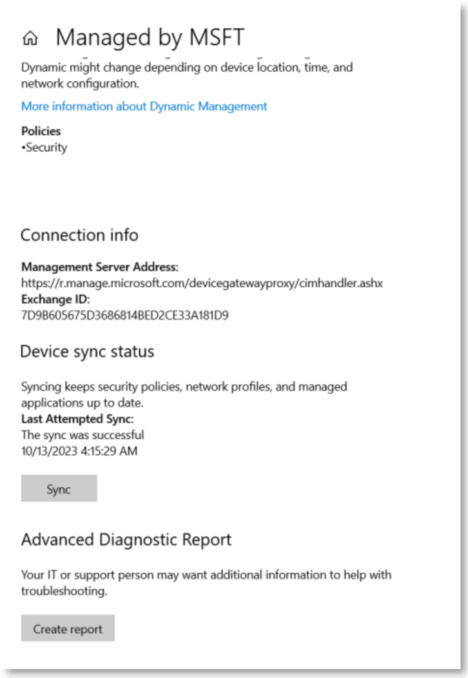
Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Connected to MSFT's Azure AD
Connected by HS@5xrbvp.onmicrosoft.com

Manage your account
Info
Disconnect
Related settings
Add or remove a provisioning package
Export your management log files
Set up an account for taking tests
Help from the web
Solving PC problems remotely
Using Remote Desktop
Configuring VPN
Get help

12. Click Sync to apply the policies to your configured Windows device.



Managed by MSFT

Dynamic might change depending on device location, time, and network configuration.

Policies
•Security

Connection info

Management Server Address:
https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx
Exchange ID:
7D9B605675D3686814BED2CE33A181D9

Device sync status

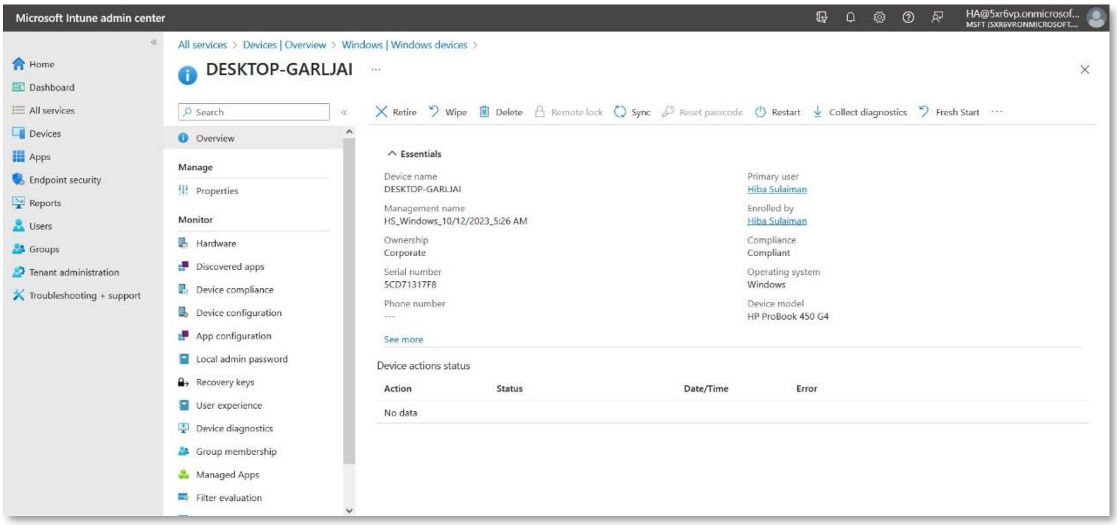
Syncing keeps security policies, network profiles, and managed applications up to date.
Last Attempted Sync:
The sync was successful
10/13/2023 4:15:29 AM

Advanced Diagnostic Report

Your IT or support person may want additional information to help with troubleshooting.

13. You can also Sync by following the steps below:
In the Microsoft Intune admin center perform the following actions:

- Click Devices from the left menu and access your Windows device.
- Click Sync to apply all the configured policies.



Device name
DESKTOP-GARLJAI

Management name
HS_Windows_10/12/2023_5:26 AM

Ownership
Corporate

Serial number
5CD71317F8

Phone number

Primary user
Hiba Sulaiman

Enrolled by
Hiba Sulaiman

Compliance
Compliant

Operating system
Windows

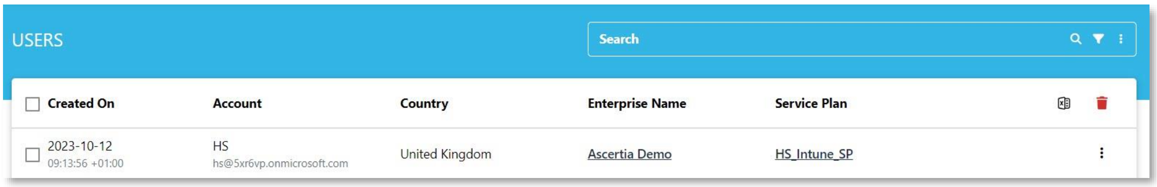
Device model
HP ProBook 450 G4

Device actions status

Action	Status	Date/Time	Error
No data			

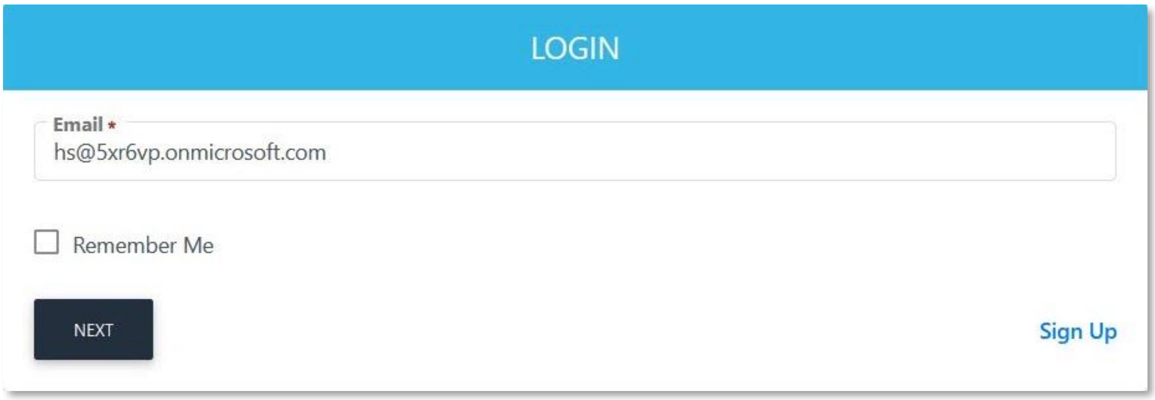
After the Sync is complete, your user will appear in the ADSS Web RA admin portal.

14. You can access ADSS Web RA to view it. From the left menu pane click Users:



□ Created On	Account	Country	Enterprise Name	Service Plan
□ 2023-10-12 09:13:56 +01:00	HS hs@5xr6vp.onmicrosoft.com	United Kingdom	Ascertia Demo	HS_Intune_SP

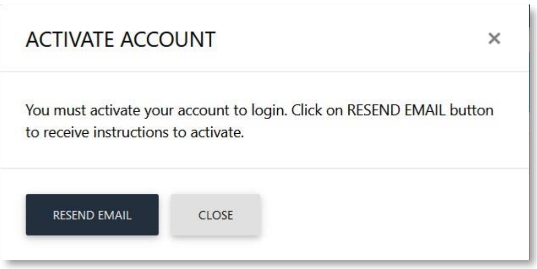
15. Then you need to sign up this user in the ADSS Web RA web portal.
Access Web RA web portal, enter your email and click Next.



Email *
hs@5xr6vp.onmicrosoft.com

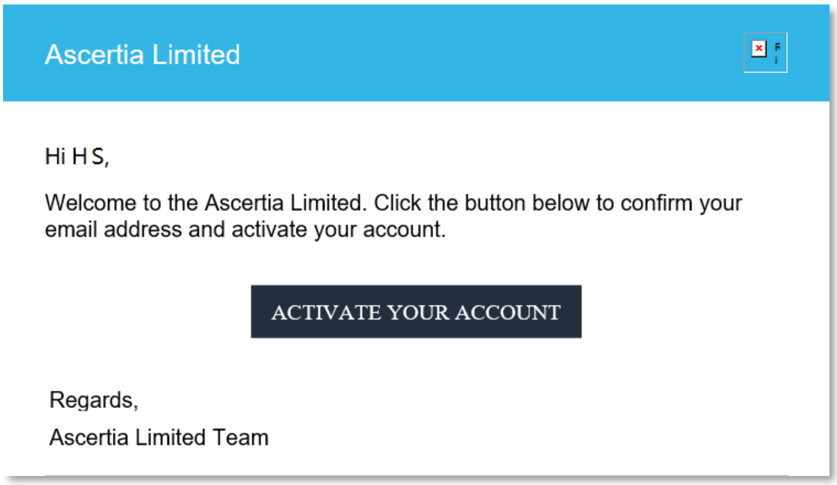
□ Remember Me

16. An account activation dialog will appear, click Resend Email.



You must activate your account to login. Click on RESEND EMAIL button to receive instructions to activate.

17. An email will be sent to the Microsoft account. Click the link in the email to complete the sign up process.



Ascertia Limited

Hi H S,

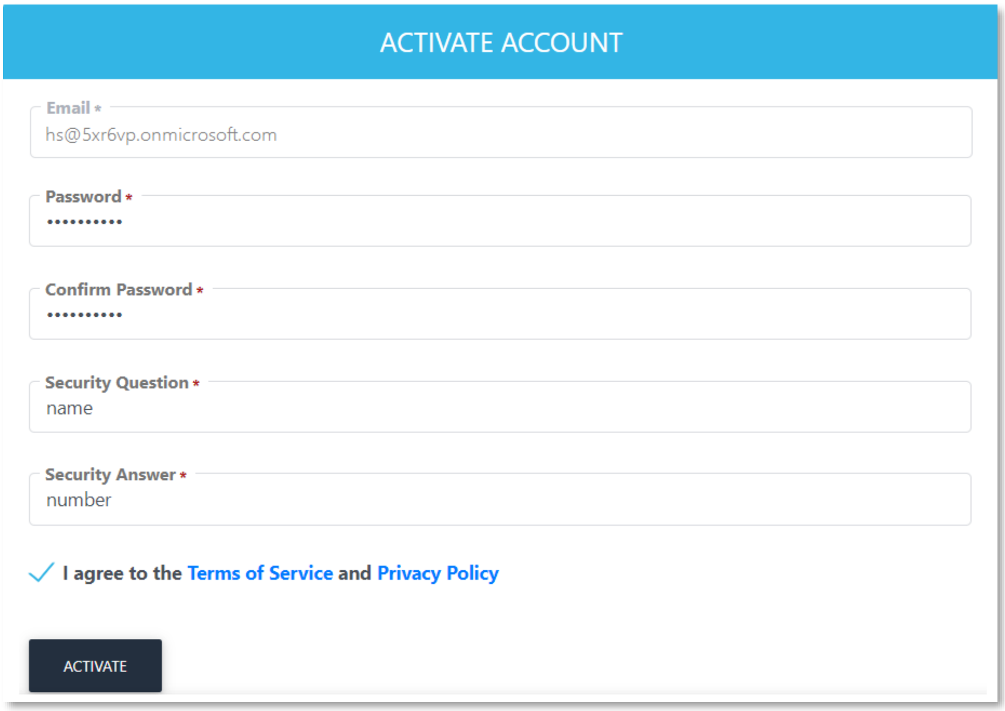
Welcome to the Ascertia Limited. Click the button below to confirm your email address and activate your account.

Regards,
Ascertia Limited Team

18. Fill the account activation details:

- Email
- Password
- Confirm Password
- Security Question
- Security Answer
- Select I agree to the Terms of Service and Privacy Policy

Click Activate.



ACTIVATE ACCOUNT

Email * hs@5xr6vp.onmicrosoft.com

Password * ••••••••••

Confirm Password * ••••••••••

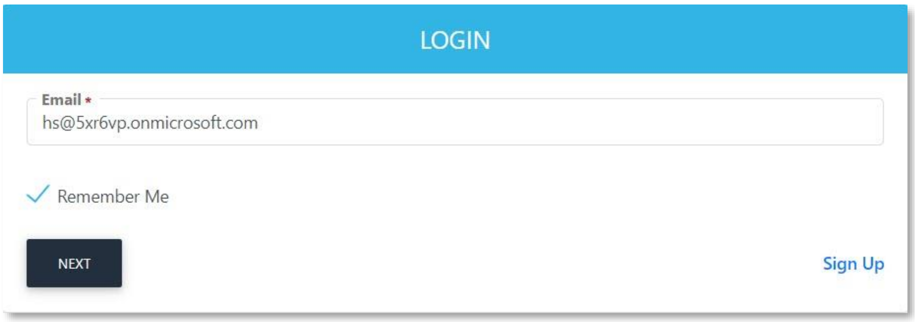
Security Question * name

Security Answer * number

✓ I agree to the Terms of Service and Privacy Policy

19. Then you will be directed to the Web RA login page.

Enter your email address, click Next.

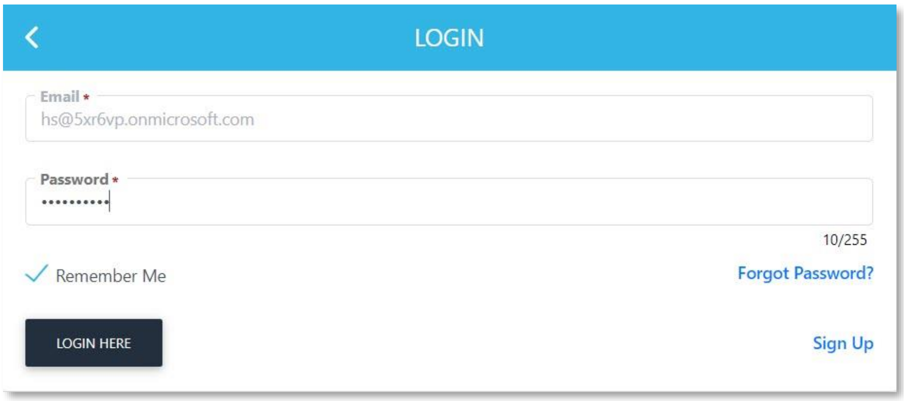


LOGIN

Email *
hs@5xr6vp.onmicrosoft.com

✓ Remember Me

20. Then enter your password and click Login here.



LOGIN

Email *
hs@5xr6vp.onmicrosoft.com

Password *
••••••••••

10/255

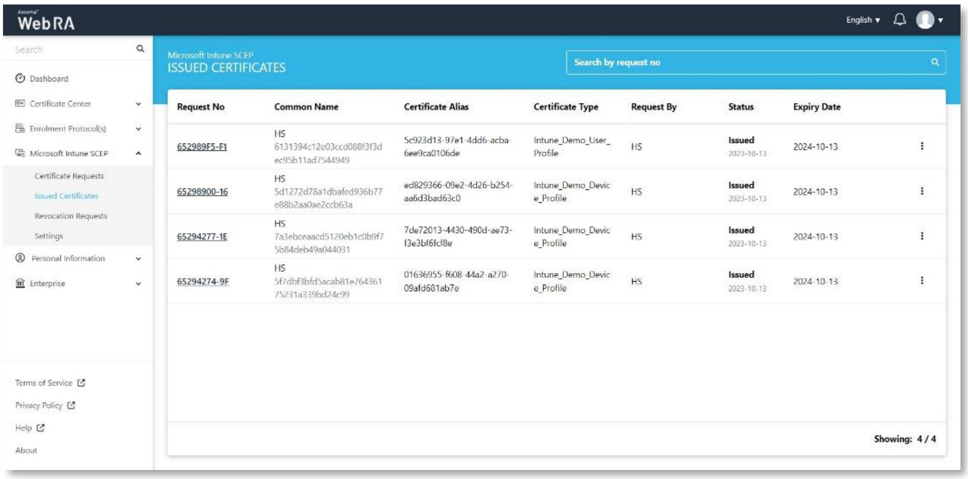
✓ Remember Me

6.3.5. Windows Sync to Generate Certificates

Once you log in to your Windows device with your user e.g. HS@5xr6vp.onmicrosoft.com, the following use cases will occur:

1. When creating user certificate, all the configured policies will be applied to the enrolled Windows devices. This may take a few minutes to apply all the policies. Once applied, they will appear in the ADSS Web RA web portal.

Access ADSS Web RA web portal > Certificates. The certificates appear in the listing.

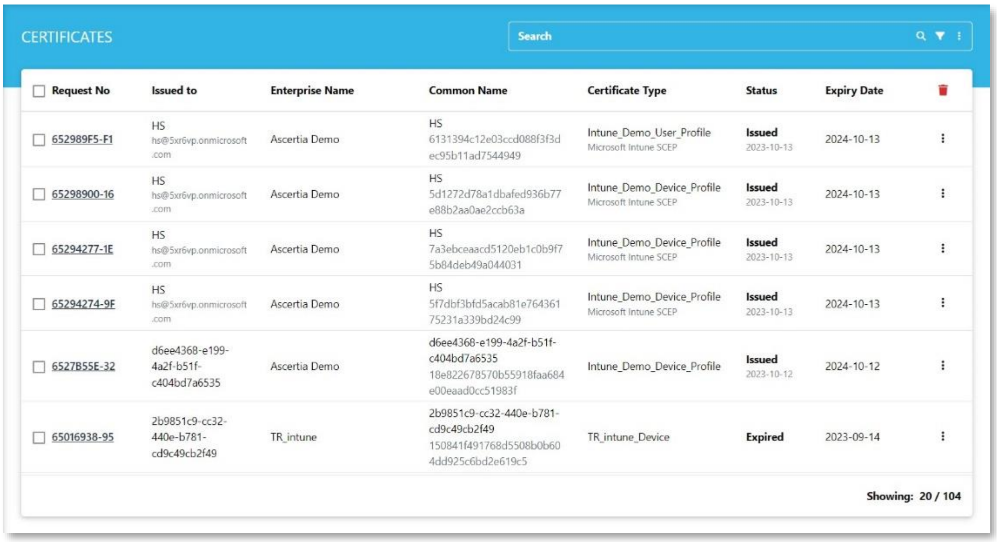


Microsoft Intune SCEP
ISSUED CERTIFICATES

Request No	Common Name	Certificate Alias	Certificate Type	Request By	Status	Expiry Date
652989F5-F1	HS 6131394c12e03ccd088f3f3dec95b11ad7544949	5c923d13-97e1-4dd6-acba-6ee9ca0106de	Intune_Demo_User_Profile	HS	Issued 2023-10-13	2024-10-13
65298900-16	HS 5d1272d78a1dbafed936b77e88b2aa0ae2ccb63a	ed829366-09e2-4d26-b254-aa6d3bad63c0	Intune_Demo_Device_Profile	HS	Issued 2023-10-13	2024-10-13
65294277-1E	HS 7a3ebceaacd5120eb1c0b9f75b84deb49a044031	7de72013-4430-490d-ae73-f3e3bf6fcf8e	Intune_Demo_Device_Profile	HS	Issued 2023-10-13	2024-10-13
65294274-9F	HS 5f7dbf3bfd5acab81e76436175231a339bd24c99	01636955-f608-44a2-a270-09afd681ab7e	Intune_Demo_Device_Profile	HS	Issued 2023-10-13	2024-10-13

Showing: 4 / 4

2. When creating a device certificate, as soon as you Sync, all the configured policies will be applied to the enrolled Windows devices automatically. Once applied, they will appear in the ADSS Web RA admin portal.



□ Request No	Issued to	Enterprise Name	Common Name	Certificate Type	Status	Expiry Date	
□ 652989F5-F1	HS hs@5xr6vp.onmicrosoft.com	Ascertia Demo	HS 6131394c12e03ccd088f3f3dec95b11ad7544949	Intune_Demo_User_Profile Microsoft Intune SCEP	Issued 2023-10-13	2024-10-13	⋮
□ 65298900-16	HS hs@5xr6vp.onmicrosoft.com	Ascertia Demo	HS 5d1272d78a1dbafed936b77e88b2aa0ae2ccb63a	Intune_Demo_Device_Profile Microsoft Intune SCEP	Issued 2023-10-13	2024-10-13	⋮
□ 65294277-1E	HS hs@5xr6vp.onmicrosoft.com	Ascertia Demo	HS 7a3ebceaacd5120eb1c0b9f75b84deb49a044031	Intune_Demo_Device_Profile Microsoft Intune SCEP	Issued 2023-10-13	2024-10-13	⋮
□ 65294274-9F	HS hs@5xr6vp.onmicrosoft.com	Ascertia Demo	HS 5f7dbf3bfd5acab81e76436175231a339bd24c99	Intune_Demo_Device_Profile Microsoft Intune SCEP	Issued 2023-10-13	2024-10-13	⋮
□ 6527B55E-32	d6ee4368-e199-4a2f-b51f-c404bd7a6535	Ascertia Demo	d6ee4368-e199-4a2f-b51f-c404bd7a6535 18e822678570b55918faa684e00eaad0cc51983f	Intune_Demo_Device_Profile	Issued 2023-10-12	2024-10-12	⋮
□ 65016938-95	2b9851c9-cc32-440e-b781-cd9c49cb2f49	TR_intune	2b9851c9-cc32-440e-b781-cd9c49cb2f49 150841f491768d5508b0b604dd925c6bd2e619c5	TR_intune_Device	Expired	2023-09-14	⋮

Showing: 20 / 104

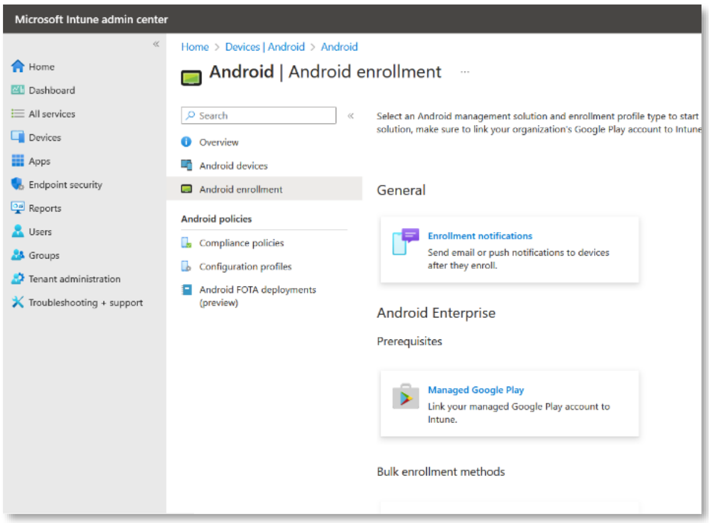
6.4. Android Enrolment for Microsoft Intune SCEP

By enrolling your device in Microsoft Intune, you get secure access to work or school apps on your Android device, and access to apps in Intune Company Portal and the Microsoft Intune app. The Company Portal app and Intune app also monitor your device settings to ensure they meet your organization's requirements and syncs including apps, policies, and updates from your organization to your device.

Firstly, you will create Android configuration policies for Trusted certificates and SCEP certificate similar to the ones created for Windows in section 6.4. Then you will proceed with the Android enrolment process.

6.4.1. Setup Android enrolment in Intune Application

1. Access the Microsoft Intune admin center.
2. From the left menu, click Devices > Android > Android enrollment.
3. Scroll to Android Enterprise and under Properties click on Managed Google Play.



Android | Android enrollment

Select an Android management solution and enrollment profile type to start solution, make sure to link your organization's Google Play account to Intune

General

Enrollment notifications
Send email or push notifications to devices after they enroll.

Android Enterprise

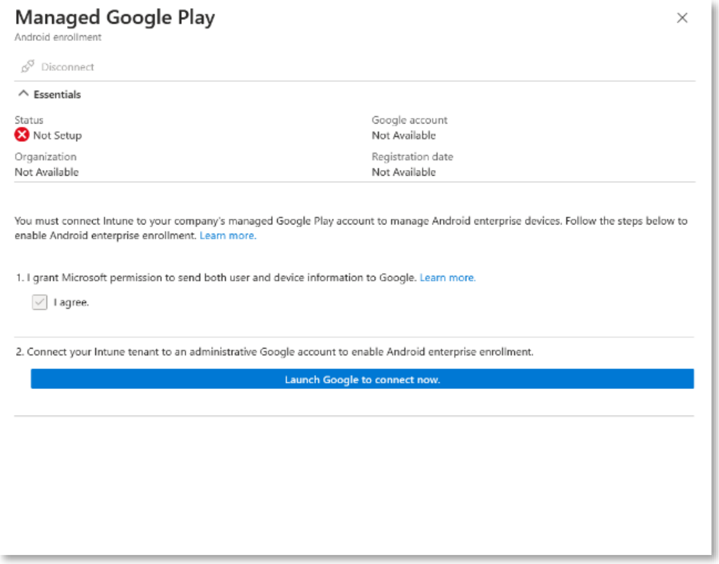
Prerequisites

Managed Google Play
Link your managed Google Play account to Intune.

Bulk enrollment methods

4. The Status of this application is Not Setup.

- Select I agree under I grant Microsoft permission to send both user and device information to Google.
- Then click Launch Google to connect now.



Managed Google Play
Android enrollment

Status
Not Setup

Google account
Not Available

Organization
Not Available

Registration date
Not Available

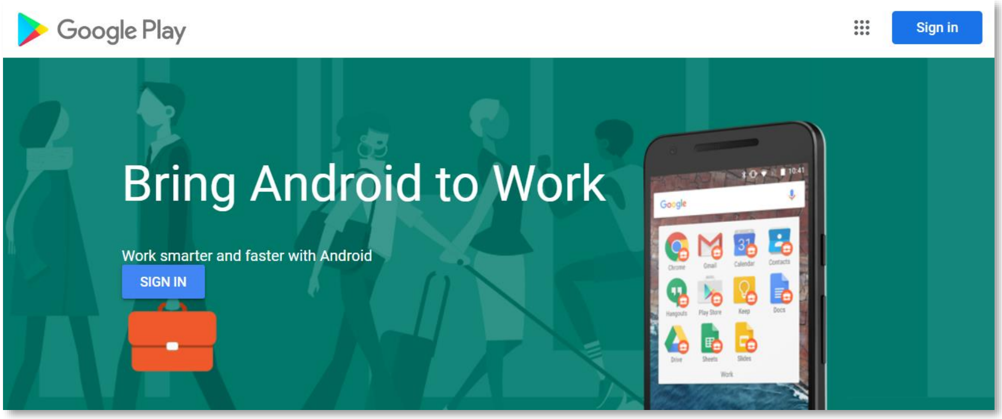
You must connect Intune to your company's managed Google Play account to manage Android enterprise devices. Follow the steps below to enable Android enterprise enrollment. Learn more.

1. I grant Microsoft permission to send both user and device information to Google. Learn more.

☑ I agree.

2. Connect your Intune tenant to an administrative Google account to enable Android enterprise enrollment.

5. Follow the wizard under the Google Play, by clicking Sign in.



Google Play

Sign in

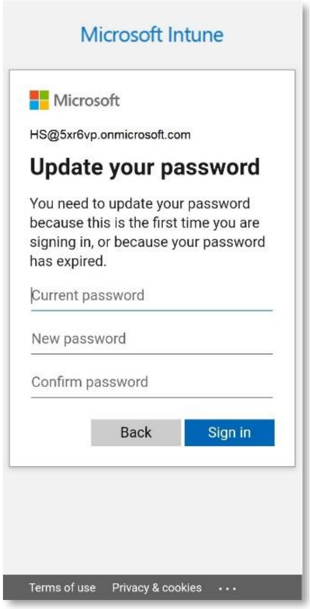
Bring Android to Work

Work smarter and faster with Android

SIGN IN

6. The following screen will appear.

Enter your current password and set a new one. Then click Sign in.



Microsoft Intune

Microsoft

HS@5xr6vp.onmicrosoft.com

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Current password

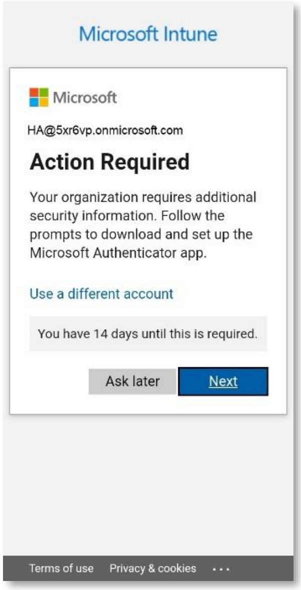
New password

Confirm password

Back | Sign in

Terms of use | Privacy & cookies | ...

7. If you have not followed the Windows enrolment for Microsoft Intune, and have not set up the Authenticator, the following will appear. Click Next.



Microsoft Intune

Microsoft

HA@5xr6vp.onmicrosoft.com

Action Required

Your organization requires additional security information. Follow the prompts to download and set up the Microsoft Authenticator app.

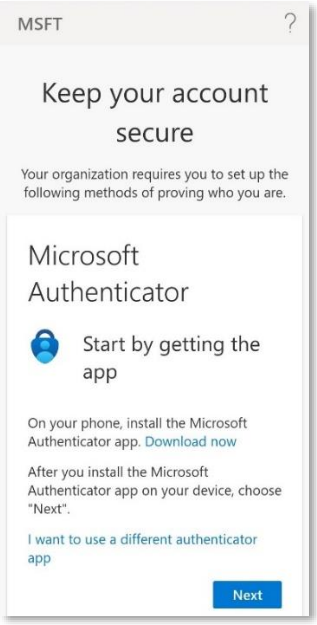
Use a different account

You have 14 days until this is required.

Ask later | Next

Terms of use | Privacy & cookies | ...

8. The Keep your account secure will appear. Click Next.



MSFT

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Start by getting the app

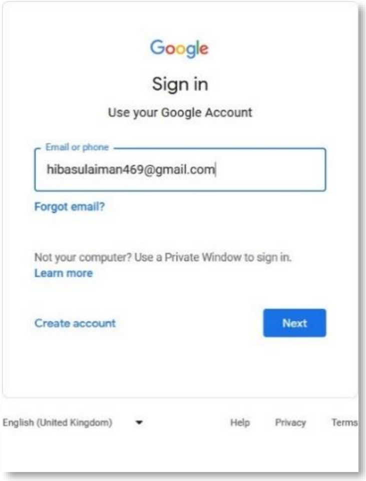
On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

9. A code will appear on your mobile’s authenticator app, enter the code, then click Next.

10. It will redirect you to Google’s log-in page.

Enter email address and click Next.



Google

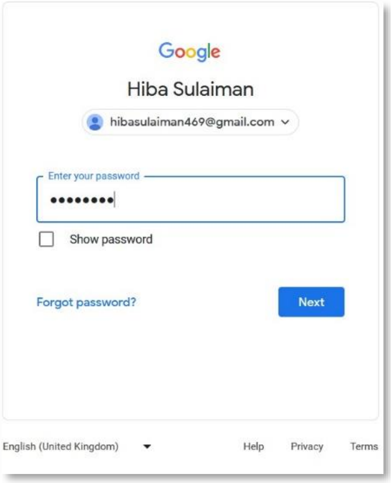
Sign in

Use your Google Account

Email or phone: hibasulaiman469@gmail.com

Not your computer? Use a Private Window to sign in.

11. Then enter password and click Next.



Google

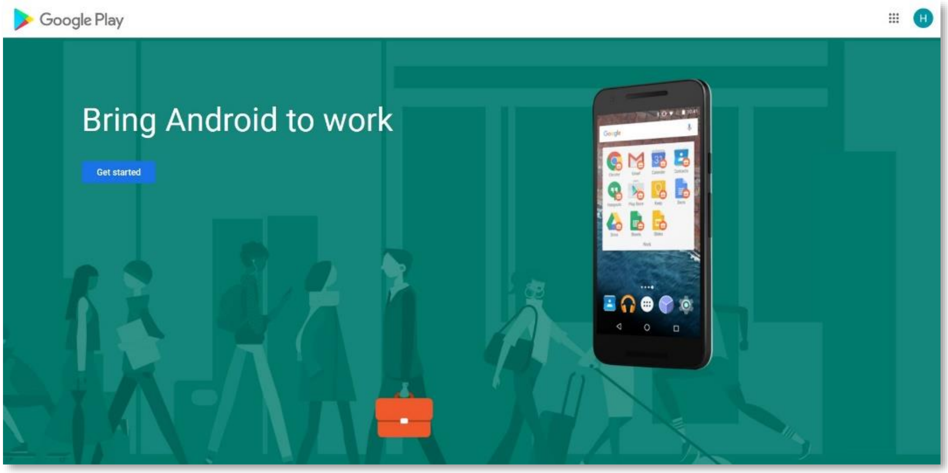
Hiba Sulaiman

hibasulaiman469@gmail.com

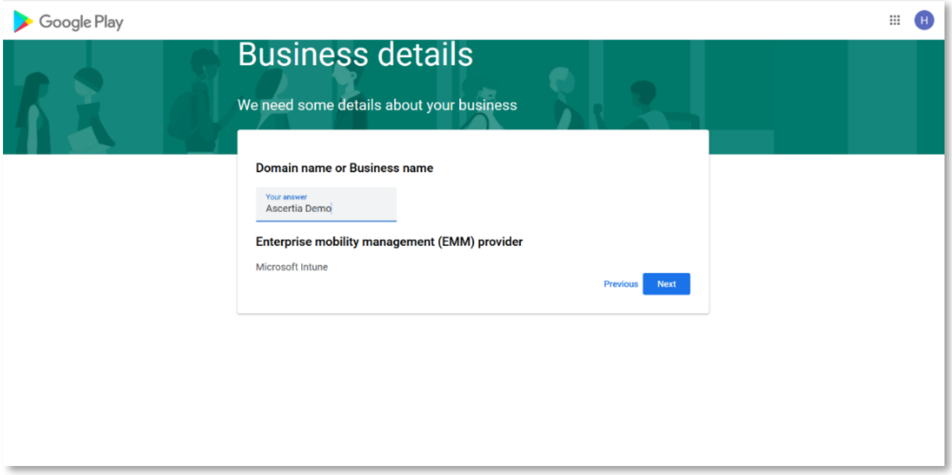
Enter your password: ••••••••

□ Show password

12. Once you log in to your Gmail account, it will redirect you to the home page. Click Get started.



13. Enter a Domain name e.g. Ascertia Demo and click Next.



Business details

We need some details about your business

Domain name or Business name

Your answer: Ascertia Demo

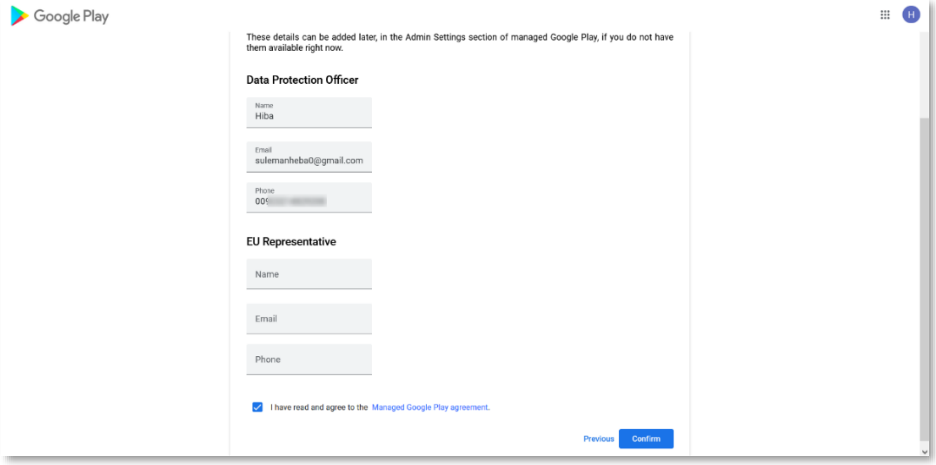
Enterprise mobility management (EMM) provider

Microsoft Intune

14. Enter the following:

- Your name
- Email
- Phone
- Select I have read and agree to the Managed Google Play agreement

Then click Confirm.



These details can be added later, in the Admin Settings section of managed Google Play, if you do not have them available right now.

Data Protection Officer

Name: Hiba

Email: sulemanheba0@gmail.com

Phone: 00[redacted]

EU Representative

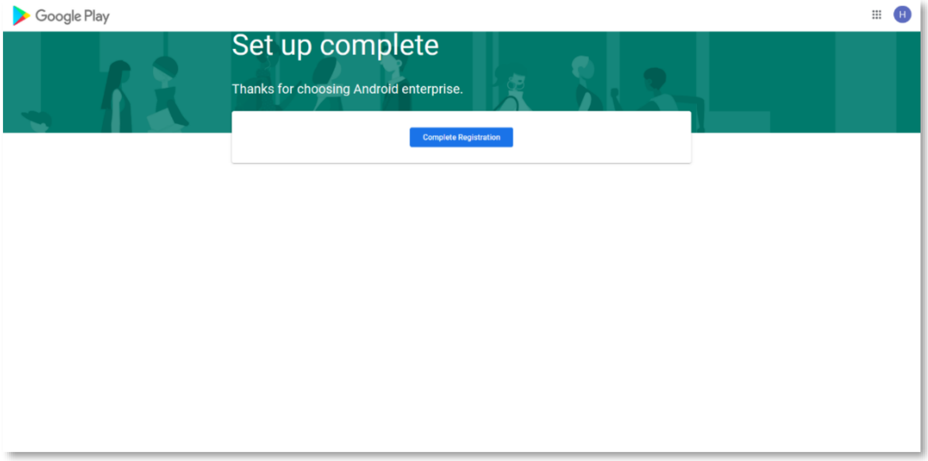
Name

Email

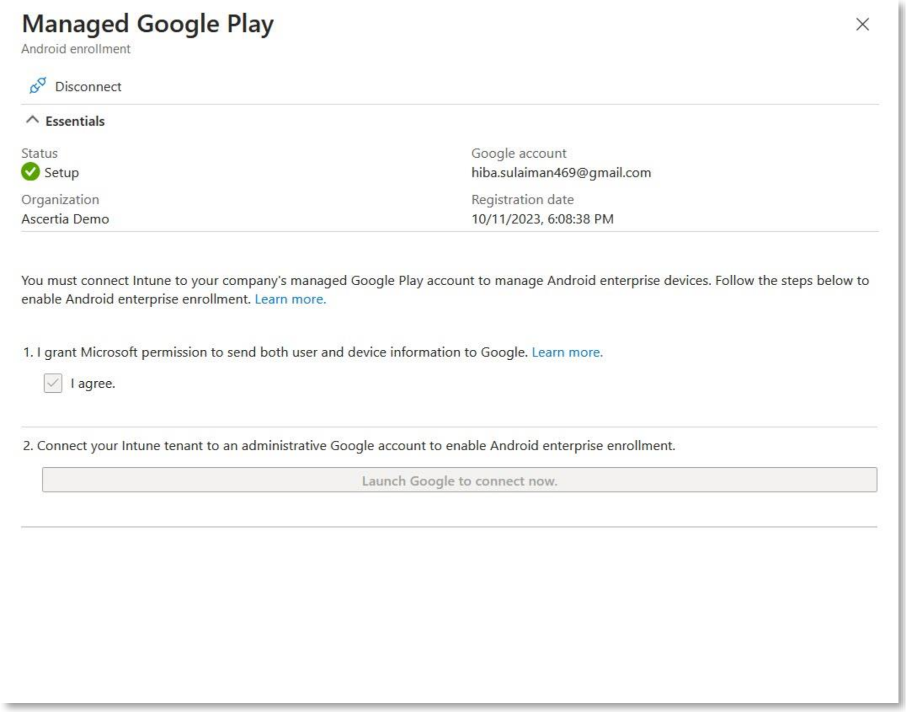
Phone

☑ I have read and agree to the Managed Google Play agreement.

15. Click Complete Registration to complete the setup.



16. Intune will redirect you to the Managed Google Play tab with the status Setup. If it does not redirect you automatically, you can switch to the Microsoft Intune admin center, the status will appear as Setup.



Managed Google Play
Android enrollment

Disconnect

Essentials

Status Setup	Google account hiba.sulaiman469@gmail.com
Organization Ascertia Demo	Registration date 10/11/2023, 6:08:38 PM

You must connect Intune to your company's managed Google Play account to manage Android enterprise devices. Follow the steps below to enable Android enterprise enrollment. Learn more.

1. I grant Microsoft permission to send both user and device information to Google. Learn more.

☑ I agree.

2. Connect your Intune tenant to an administrative Google account to enable Android enterprise enrollment.

Launch Google to connect now.

17. Once the device enrolment is compete, you have to enrol your Android device on the Company Portal app.

6.4.2. Enrol your Android device with Company Portal

Enrol your personal or corporate-owned Android device with Intune Company Portal to get secure access to company email, apps, and data. Use the same Gmail account to log in to this application that you have used in Microsoft Intune.

Company Portal supports devices running Android 8.0 and later.

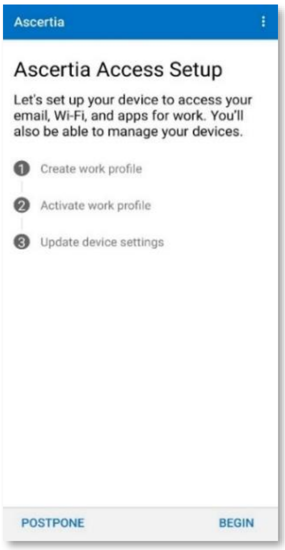
Install Company Portal application

1. On your Android device, tap Home, then tap Play Store.
2. Search for and install Intune Company Portal.
3. Tap Accept, when app permissions prompt.

Enrol Device

During enrolment, when prompted, choose a category that best describes how you use your device.

1. Open the Company Portal app and sign in with your work account. If prompted to, review notification permissions for the application.
2. If prompted to accept organization’s terms and conditions, tap Accept All.
3. Tap Begin to enrol your device.

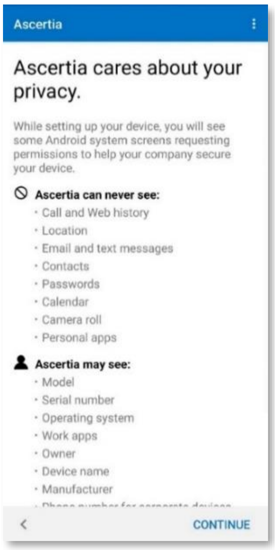


Ascertia Access Setup

Let’s set up your device to access your email, Wi-Fi, and apps for work. You’ll also be able to manage your devices.

1. Create work profile
2. Activate work profile
3. Update device settings

4. Review what your organization can and cannot see. Then tap Continue.



Ascertia cares about your privacy.

While setting up your device, you will see some Android system screens requesting permissions to help your company secure your device.

Ascertia can never see:

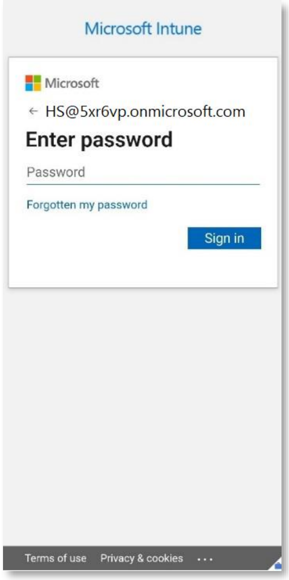
- Call and Web history
- Location
- Email and text messages
- Contacts
- Passwords
- Calendar
- Camera roll
- Personal apps

Ascertia may see:

- Model
- Serial number
- Operating system
- Work apps
- Owner
- Device name
- Manufacturer
- Phone number for corporate devices

5. Log in to your Microsoft Intune account by:

- Entering your email e.g. HS@5xr6vp.onmicrosoft.com
- Password
- Then click Sign in.



Microsoft Intune

Microsoft

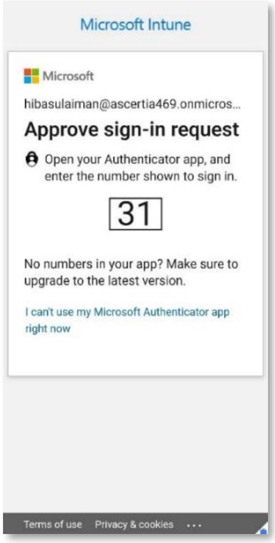
← HS@5xr6vp.onmicrosoft.com

Enter password

Password

Forgotten my password

6. Login to the Authenticator app and sign-in with your Microsoft Intune user credentials. Open the Authenticator app on your device and approve with the prompted verification code. Refer to section 6.1 point 4 to see the Microsoft Authenticator configurations.



Microsoft Intune

Microsoft

hibasulaiman@ascertia469.onmicros...

Approve sign-in request

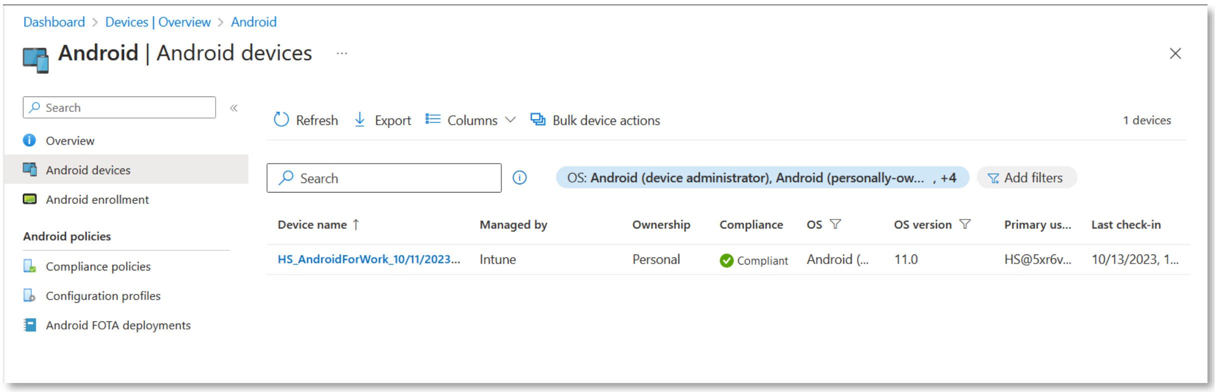
Open your Authenticator app, and enter the number shown to sign in.

31

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

7. Your device is enrolled in the Microsoft Intune admin center.



Dashboard > Devices | Overview > Android

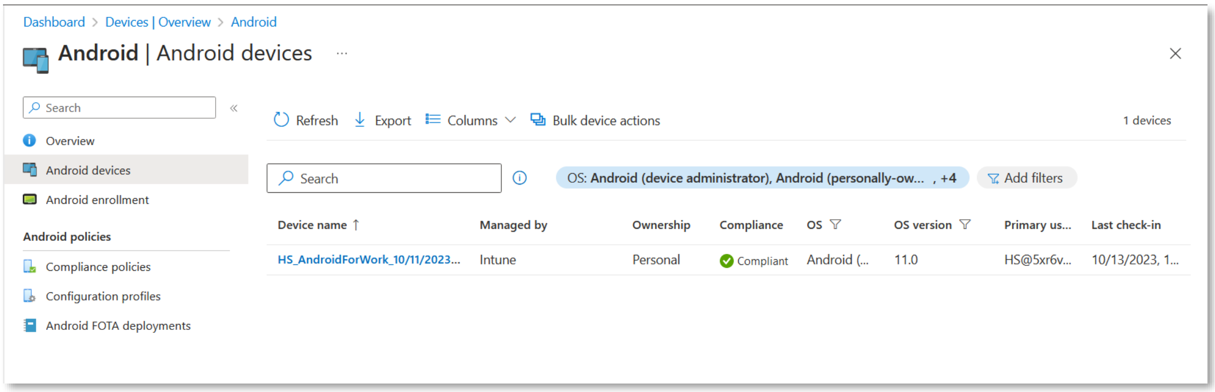
Android | Android devices ...

1 devices

OS: Android (device administrator), Android (personally-ow... , +4

Device name ↑	Managed by	Ownership	Compliance	OS	OS version	Primary us...	Last check-in
HS_AndroidForWork_10/11/2023...	Intune	Personal	✓ Compliant	Android (...	11.0	HS@5xr6v...	10/13/2023, 1...

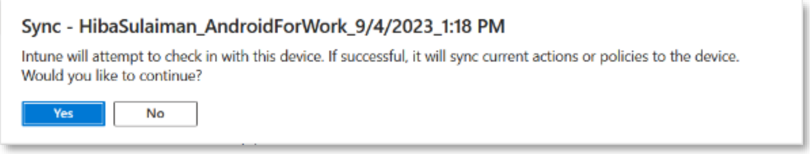
8. Click on the device, all the details of the device will be displayed.



Device name ↑	Managed by	Ownership	Compliance	OS	OS version	Primary us...	Last check-in
HS_AndroidForWork_10/11/2023...	Intune	Personal	✓ Compliant	Android (...	11.0	HS@5xr6v...	10/13/2023, 1...

6.4.3. Android Sync to Generate Certificates

1. Once your Google account is linked with Intune, click Sync to apply all the policies and updates.



Sync - HibaSulaiman_AndroidForWork_9/4/2023_1:18 PM

Intune will attempt to check in with this device. If successful, it will sync current actions or policies to the device. Would you like to continue?

2. Now, you can Sync via Company Portal app or from the Microsoft Intune admin center as explained above, to apply all the profiles you have created for your Android device. Once the policies are applied, your certificates can be viewed from the ADSS Web RA admin or web portal (depending on the type of certificates i.e. User or device).

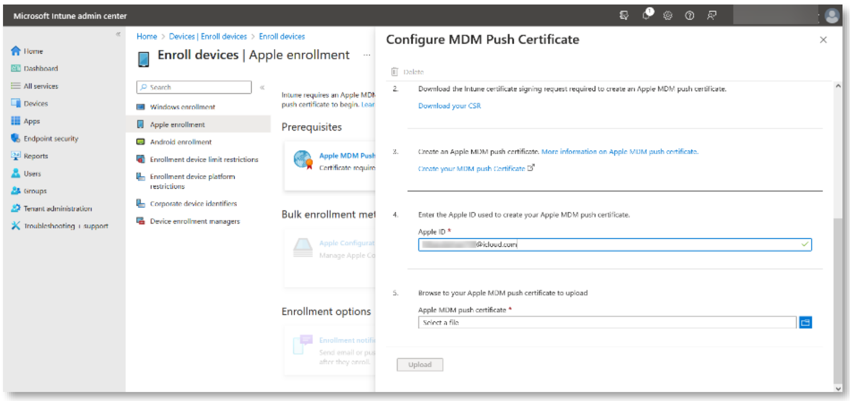
6.5. iOS Enrolment for Microsoft Intune SCEP

Enrol your iOS device with the Intune Company Portal app to gain secure access to your organization's email, files, and apps.

After your device is enrolled, it becomes managed. Your organization can assign policies and apps to the device through a mobile device management (MDM) provider, such as Intune.

6.5.1. Setup iOS Enrolment in Intune Application

1. From the left menu, click Devices > iOS/iPadOS > iOS/iPadOS enrollment. From the Prerequisites, click Apple MDM push Certificate. Select I grant Microsoft permission to send both user and device information to Apple.



Enroll devices | Apple enrollment

Intune requires an Apple MDM push certificate to begin. Lear

Apple MDM Push Certificate require

Manage Apple Co

Send email or pu after they enroll.

Configure MDM Push Certificate

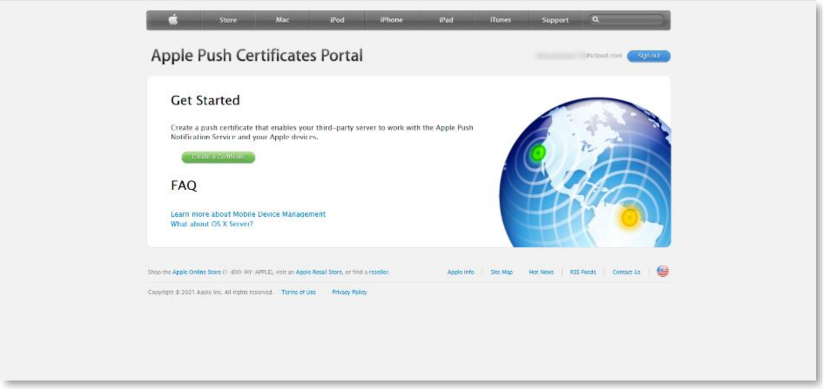
2. Download the Intune certificate signing request required to create an Apple MDM push certificate.
   Download your CSR

3. Create an Apple MDM push certificate. More information on Apple MDM push certificate.
   Create your MDM push Certificate

4. Enter the Apple ID used to create your Apple MDM push certificate.
   Apple ID *: [redacted]@icloud.com

5. Browse to your Apple MDM push certificate to upload
   Apple MDM push certificate *: Select a file

2. Download the Intune certificate-signing request.
3. Then create an Apple MDM push certificate. Click the link; it will redirect you to the Apple (Idms) portal. Login with your Apple ID.



Apple Push Certificates Portal

[redacted]@icloud.com

Get Started

Create a push certificate that enables your third-party server to work with the Apple Push Notification Service and your Apple devices.

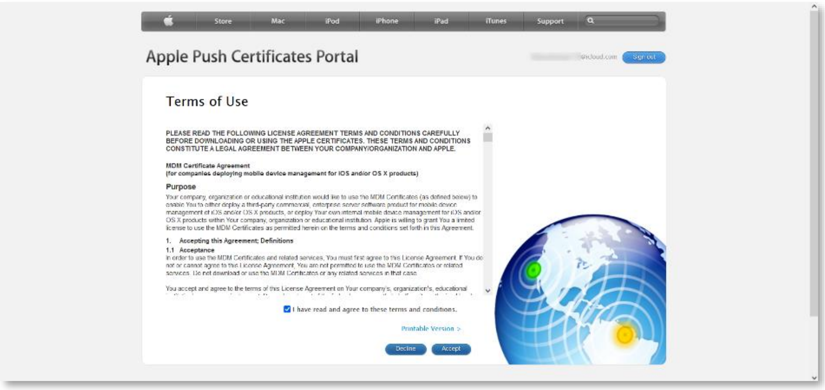
FAQ

Learn more about Mobile Device Management
What about OS X Server?

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Copyright © 2021 Apple Inc. All rights reserved.

4. At the Terms of Use, select I have read and agree to these terms and conditions, and click Accept.



Apple Push Certificates Portal

[redacted]@icloud.com

Terms of Use

PLEASE READ THE FOLLOWING LICENSE AGREEMENT TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING OR USING THE APPLE CERTIFICATES. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOUR COMPANY/ORGANIZATION AND APPLE.

MDM Certificate Agreement
(for companies deploying mobile device management for iOS and/or OS X products)

Purpose

Your company, organization or educational institution would like to use the MDM Certificates (as defined below) to enable You to either deploy a third-party commercial, enterprise server software product for mobile device management of iOS and/or OS X products, or deploy Your own internal mobile device management for iOS and/or OS X products within Your company, organization or educational institution. Apple is willing to grant You a limited license to use the MDM Certificates as permitted herein on the terms and conditions set forth in this Agreement.

1. Accepting this Agreement; Definitions

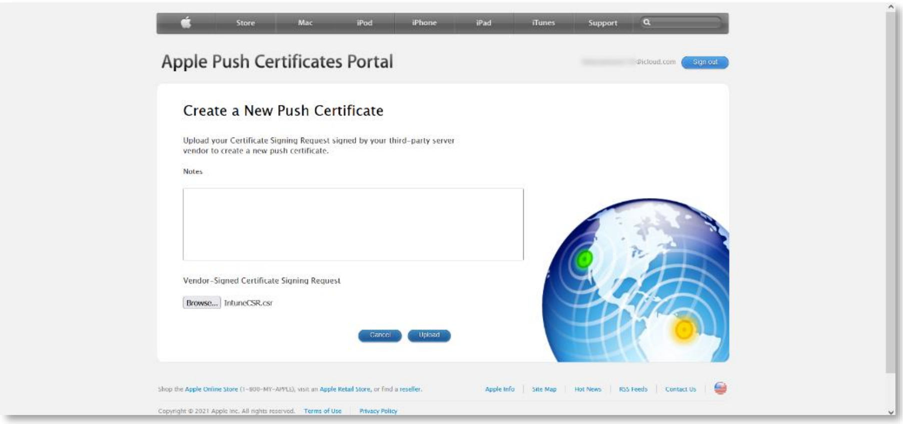
1.1 Acceptance

In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any related services in that case.

You accept and agree to the terms of this License Agreement on Your company's, organization's, educational

☑ I have read and agree to these terms and conditions.

5. In the next step, upload the CSR you downloaded in step 3, and click Upload.



Apple Push Certificates Portal

[redacted]@icloud.com Sign out

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

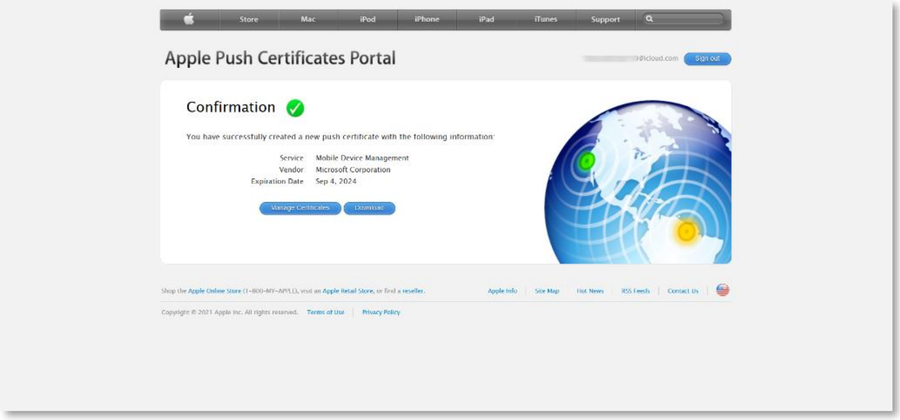
Browse... IntuneCSR.csr

Cancel Upload

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller. Apple Info | Site Map | Hot News | RSS Feeds | Contact Us

Copyright © 2021 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

6. The confirmation screen will appear, where you can manage certificates or download it.



Apple Push Certificates Portal

[redacted]@icloud.com Sign out

Confirmation ✓

You have successfully created a new push certificate with the following information:

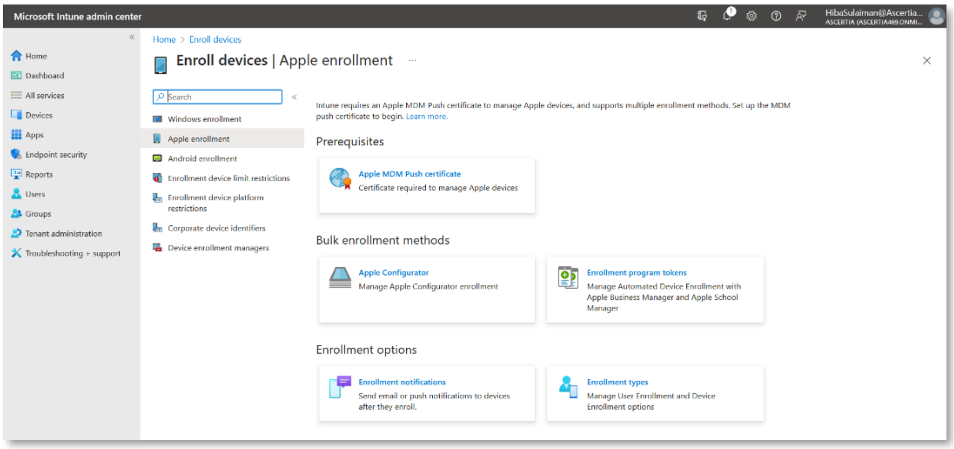
Service	Mobile Device Management
Vendor	Microsoft Corporation
Expiration Date	Sep 4, 2024

Manage Certificates Download

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller. Apple Info | Site Map | Hot News | RSS Feeds | Contact Us

Copyright © 2021 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

7. In the Microsoft Intune admin center, enter your Apple ID.
8. Upload your Apple MDM push certificate and then click Upload. Once the upload is complete, all the enrolment methods will be enabled.



Microsoft Intune admin center
HibaSulaiman@Ascertia...
ASCERTIA (ASCERTIA469.ONMI...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Enroll devices
Search
Windows enrollment
Apple enrollment
Android enrollment
Enrollment device limit restrictions
Enrollment device platform restrictions
Corporate device identifiers
Device enrollment managers

Enroll devices | Apple enrollment

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. Learn more.

Prerequisites

Apple MDM Push certificate
Certificate required to manage Apple devices

Bulk enrollment methods

Apple Configurator
Manage Apple Configurator enrollment

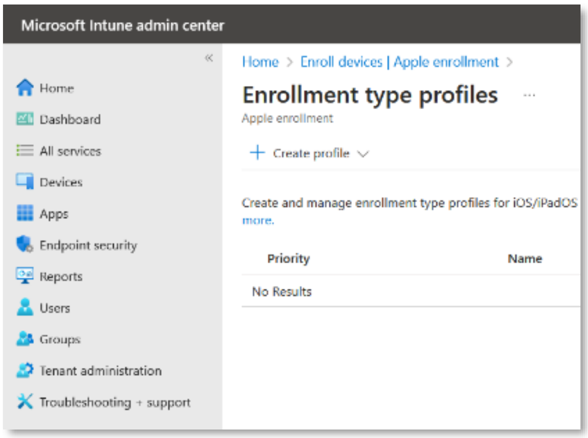
Enrollment program tokens
Manage Automated Device Enrollment with Apple Business Manager and Apple School Manager

Enrollment options

Enrollment notifications
Send email or push notifications to devices after they enroll.

Enrollment types
Manage User Enrollment and Device Enrollment options

9. From the Enrolment Options, click Enrolment Types. Then click Create profile. Select iOS/ iPadOS.


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Enroll devices | Apple enrollment >

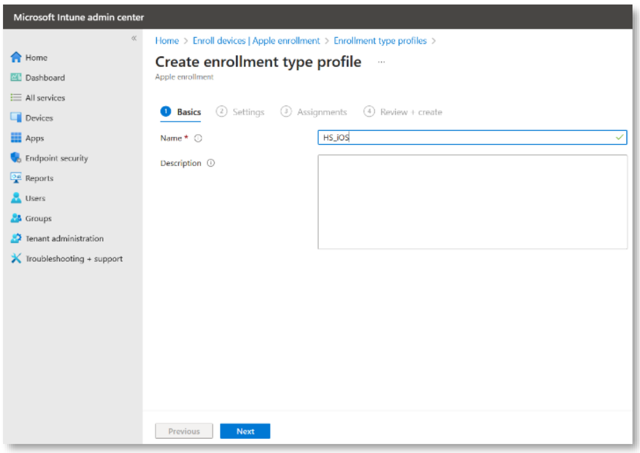
Enrollment type profiles

Apple enrollment

Create and manage enrollment type profiles for iOS/iPadOS
more.

Priority	Name
No Results	

10. In the Basics tab, set a profile name for the iOS Certificate e.g. HS_iOS. Then click Next.



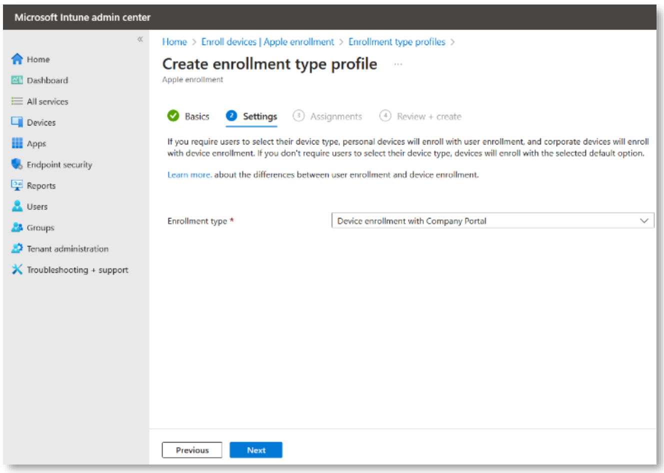
Create enrollment type profile

Apple enrollment

Name * HS_iOS

Description

11. In the Settings tab, select Device enrolment with Company Portal from the drop down, and click Next.



Create enrollment type profile

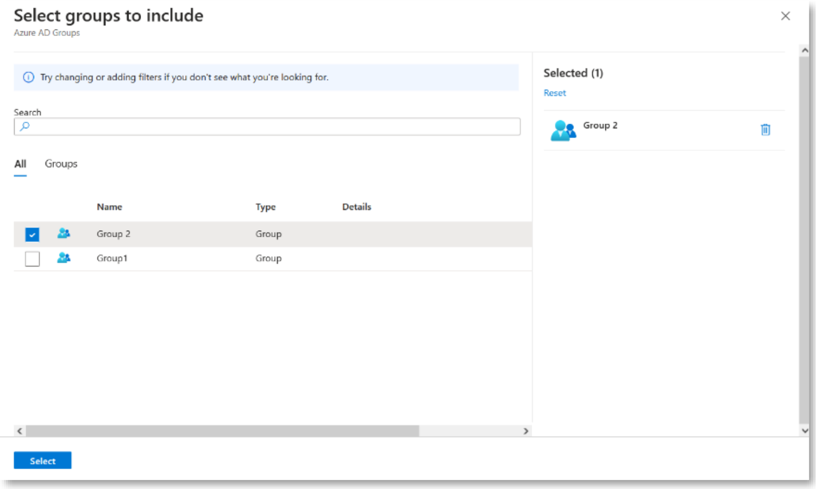
Apple enrollment

If you require users to select their device type, personal devices will enroll with user enrollment, and corporate devices will enroll with device enrollment. If you don't require users to select their device type, devices will enroll with the selected default option.

Learn more. about the differences between user enrollment and device enrollment.

Enrollment type * Device enrollment with Company Portal

12. In the Assignments tab, click Add groups, then select your relevant group e.g. Group 2 and click Select.



Select groups to include
Azure AD Groups

Try changing or adding filters if you don't see what you're looking for.

Search

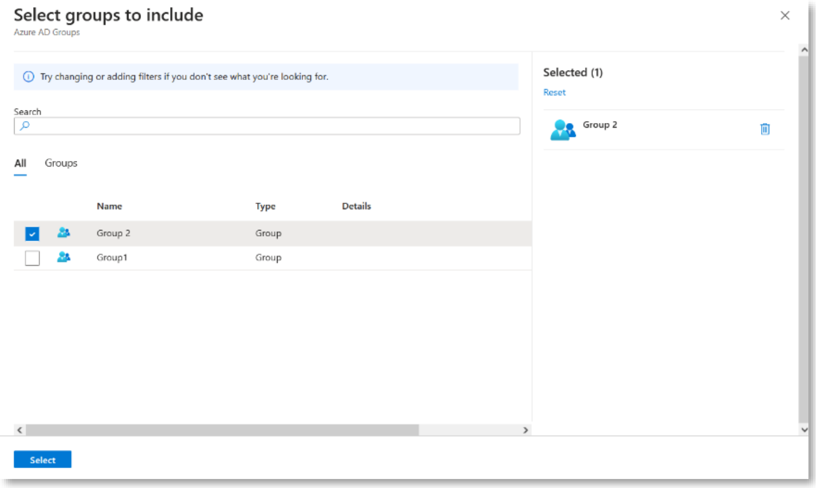
All Groups

		Name	Type	Details
☑		Group 2	Group	
□		Group1	Group	

Selected (1)
Reset
Group 2

Select

13. The group will be added to the list of Included groups.



Select groups to include
Azure AD Groups

Try changing or adding filters if you don't see what you're looking for.

Search

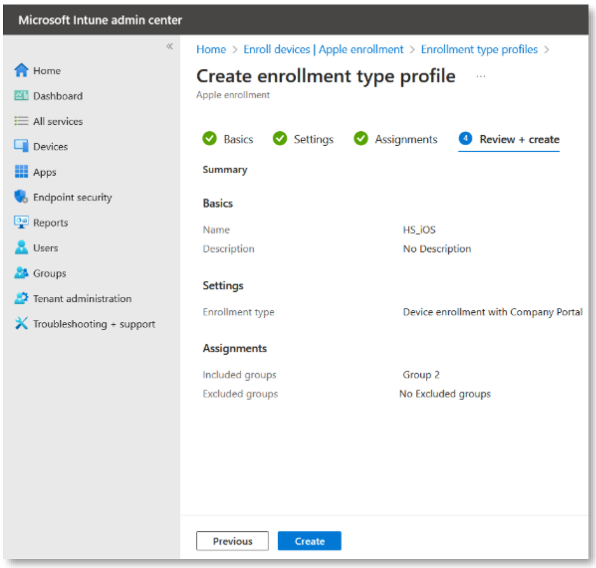
All Groups

		Name	Type	Details
☑		Group 2	Group	
□		Group1	Group	

Selected (1)
Reset
Group 2

Select

14. On the Review + create tab, click Create.



Microsoft Intune admin center

Home > Enroll devices | Apple enrollment > Enrollment type profiles >

Create enrollment type profile
Apple enrollment

Basics Settings Assignments Review + create

Summary

Basics

Name	HS_iOS
Description	No Description

Settings

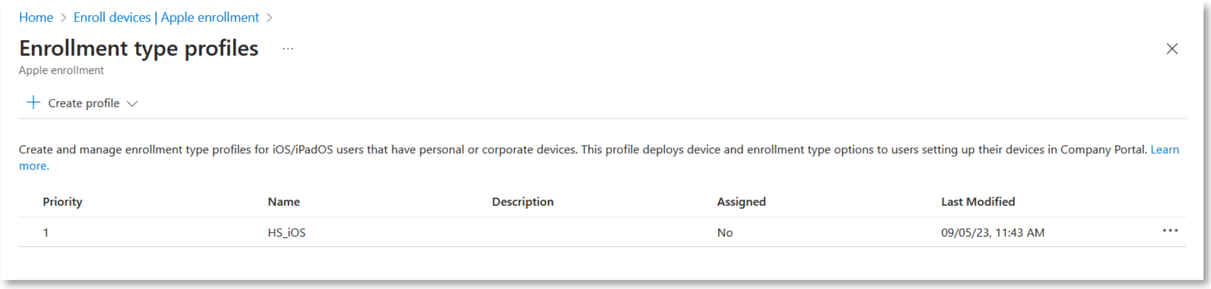
Enrollment type	Device enrollment with Company Portal

Assignments

Included groups	Group 2
Excluded groups	No Excluded groups

Previous Create

15. The profile you created will be listed in the enrolment type profiles listing.



Home > Enroll devices | Apple enrollment >

Enrollment type profiles

Apple enrollment

Create and manage enrollment type profiles for iOS/iPadOS users that have personal or corporate devices. This profile deploys device and enrollment type options to users setting up their devices in Company Portal. Learn more.

Priority	Name	Description	Assigned	Last Modified
1	HS_iOS		No	09/05/23, 11:43 AM

Once the device enrolment is compete, you have to enrol your iOS device on the Company Portal app.

6.5.2. Enrol your iOS device with Company Portal

Enrol your personal or corporate-owned iOS device with Intune Company Portal to get secure access to company email, apps, and data.

Company Portal supports devices running iOS 14.0 and later.

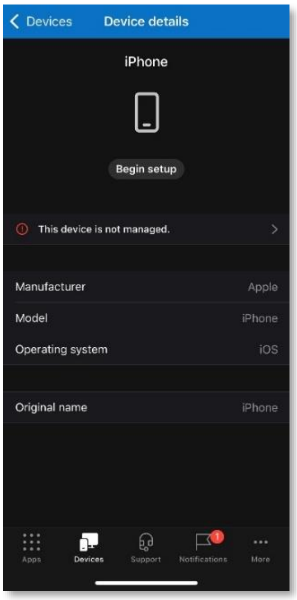
Install Company Portal application

1. On your iOS device, tap Home, then tap App Store.
2. Search for and install Intune Company Portal.
3. Tap Accept, when app permissions prompt.

Enrol Device

During enrolment, when prompted, choose a category that best describes how you use your device.

1. Open the Company Portal app and sign in with your work account. If prompted to, review notification permissions for the application.
2. If prompted to accept organization’s terms and conditions, tap Accept All.
3. Tap Begin setup to enrol your device.



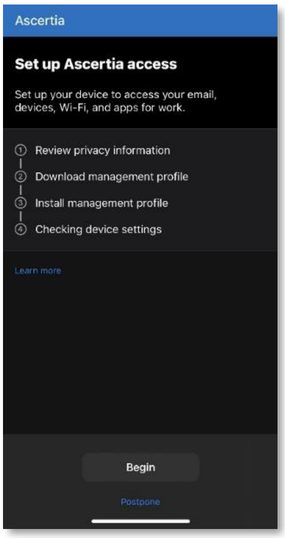
Device details

iPhone

This device is not managed.

Manufacturer	Apple
Model	iPhone
Operating system	iOS
Original name	iPhone

4. From the set up organization access screen, tap Begin.



Ascertia

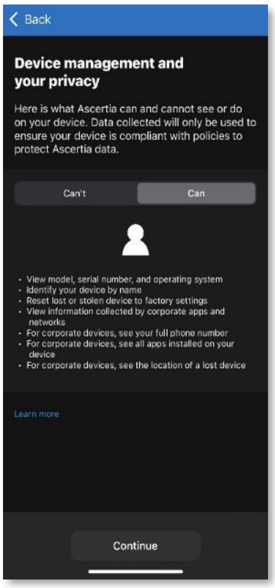
Set up Ascertia access

Set up your device to access your email, devices, Wi-Fi, and apps for work.

1. Review privacy information
2. Download management profile
3. Install management profile
4. Checking device settings

Learn more

5. Review what your organization can and cannot see. Then tap Continue.



Back

Device management and your privacy

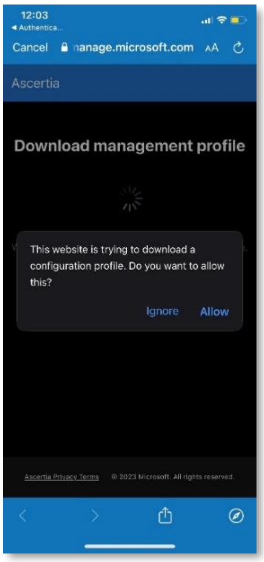
Here is what Ascertia can and cannot see or do on your device. Data collected will only be used to ensure your device is compliant with policies to protect Ascertia data.

Can't | Can

- View model, serial number, and operating system
- Identify your device by name
- Reset lost or stolen device to factory settings
- View information collected by corporate apps and networks
- For corporate devices, see your full phone number
- For corporate devices, see all apps installed on your device
- For corporate devices, see the location of a lost device

Learn more

6. If prompted to, allow permissions to download a configuration profile.



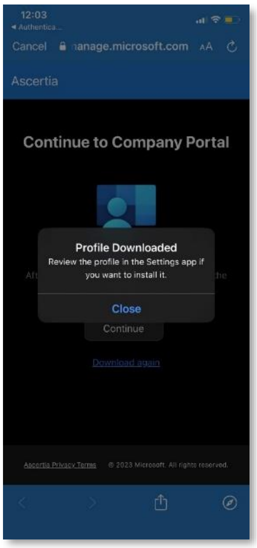
Ascertia

Download management profile

This website is trying to download a configuration profile. Do you want to allow this?

Ascertia Privacy Terms © 2023 Microsoft. All rights reserved.

7. Once the profile is downloaded, the following confirmation message will pop-up, tap Close.

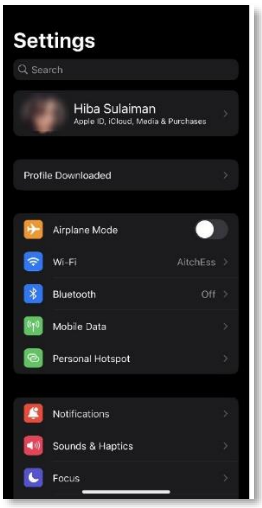


Profile Downloaded

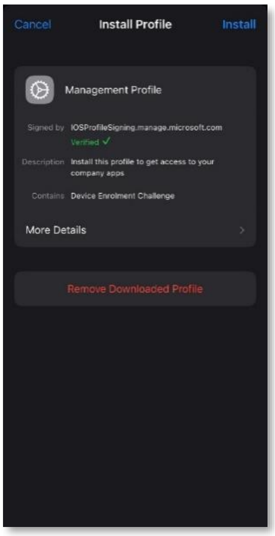
Review the profile in the Settings app if you want to install it.

© 2023 Microsoft. All rights reserved.

8. Then go to your iOS device's Settings. Under the Apple ID, tap Profile Downloaded.



9. The configured management profile will be enabled, tap Install to proceed.

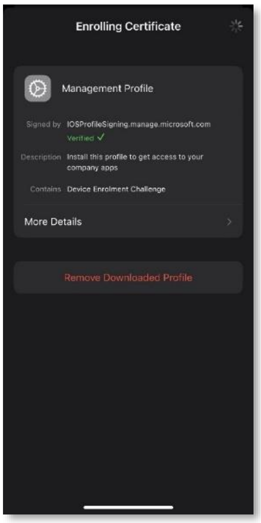


Signed by IOSProfileSigning.manage.microsoft.com
Verified ✓

Description Install this profile to get access to your company apps

Contains Device Enrolment Challenge

10. While enrolling the certificate, the following will appear.

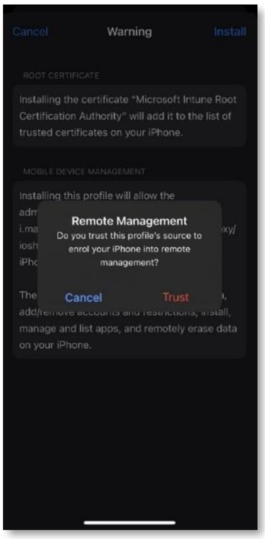


Signed by IOSProfileSigning.manage.microsoft.com
Verified ✓

Description Install this profile to get access to your company apps

Contains Device Enrolment Challenge

11. When prompted, tap Trust to enrol your iOS device into remote management.



Installing the certificate "Microsoft Intune Root Certification Authority" will add it to the list of trusted certificates on your iPhone.

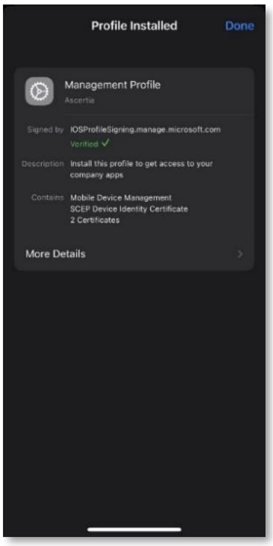
Installing this profile will allow the adm
i.ma xy/
iosh
iPhc

The
add/remove accounts and restrictions, install, manage and list apps, and remotely erase data on your iPhone.

Remote Management

Do you trust this profile's source to enrol your iPhone into remote management?

12. Once the profile is installed, tap Done. Open the Company Portal app again.

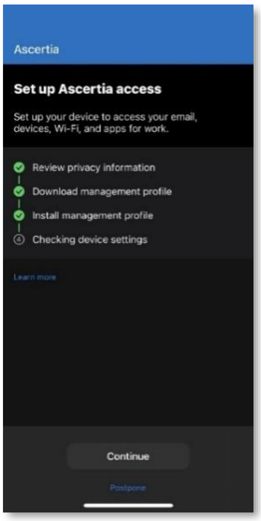


Signed by IOSProfileSigning.manage.microsoft.com
Verified ✓

Description Install this profile to get access to your company apps

Contains Mobile Device Management
SCEP Device Identity Certificate
2 Certificates

13. The set up organization access screen will appear, tap Continue.



Ascertia

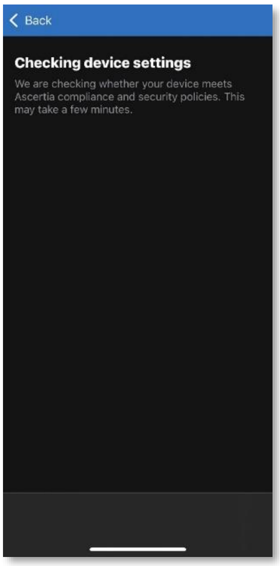
Set up Ascertia access

Set up your device to access your email, devices, Wi-Fi, and apps for work.

- Review privacy information
- Download management profile
- Install management profile
- Checking device settings

Learn more

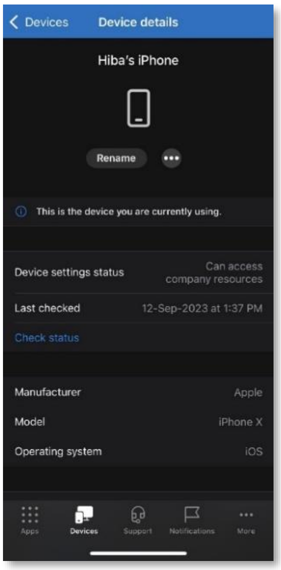
14. The app will check the device settings. This may take some time.



Checking device settings

We are checking whether your device meets Ascertia compliance and security policies. This may take a few minutes.

15. Once your device in enrolled, your device details will appear.



Hiba's iPhone

This is the device you are currently using.

Device settings status: Can access company resources

Last checked: 12-Sep-2023 at 1:37 PM

Check status

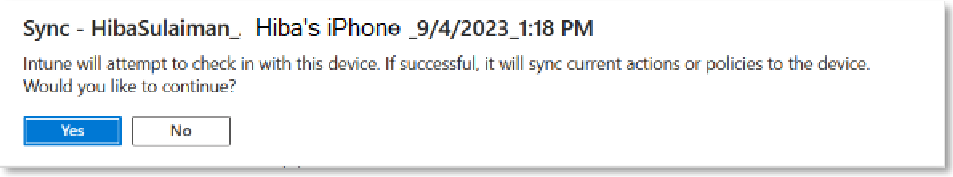
Manufacturer: Apple

Model: iPhone X

Operating system: iOS

6.5.3. iOS Sync to Generate Certificates

1. Once your iOS device is linked with Intune, in the list of devices you manage, select the iOS device to open its Overview pane, and then select Sync.



Sync - HibaSulaiman_ Hiba's iPhone _9/4/2023_1:18 PM

Intune will attempt to check in with this device. If successful, it will sync current actions or policies to the device. Would you like to continue?

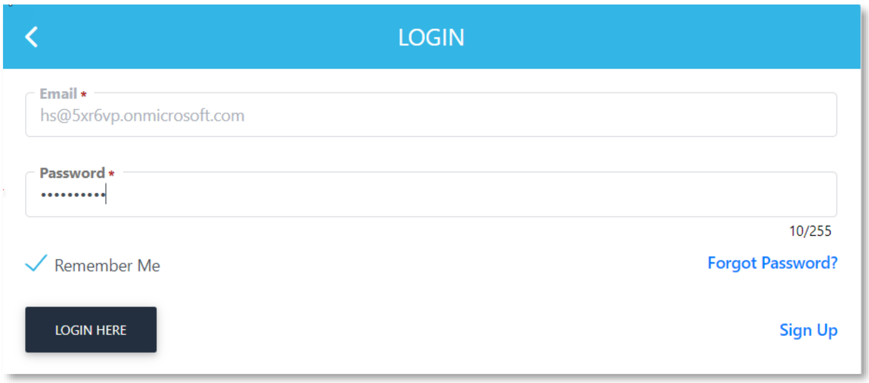
2. To confirm, select Yes.

You can Sync via Company Portal app or from the Microsoft Intune admin center as explained above, to apply all the profiles you have created for your Android device. Once the policies are applied, your certificates can be viewed from the ADSS Web RA admin or web portal (depending on the type of certificates i.e. User or device).

7. View Certificates (from ADSS Web RA Web Portal)

The Microsoft Intune user can view and manage the certificates from ADSS Web RA web portal.

1. Log in to ADSS Web RA web portal using your Microsoft Intune user credentials.



LOGIN

Email * hs@5xr6vp.onmicrosoft.com

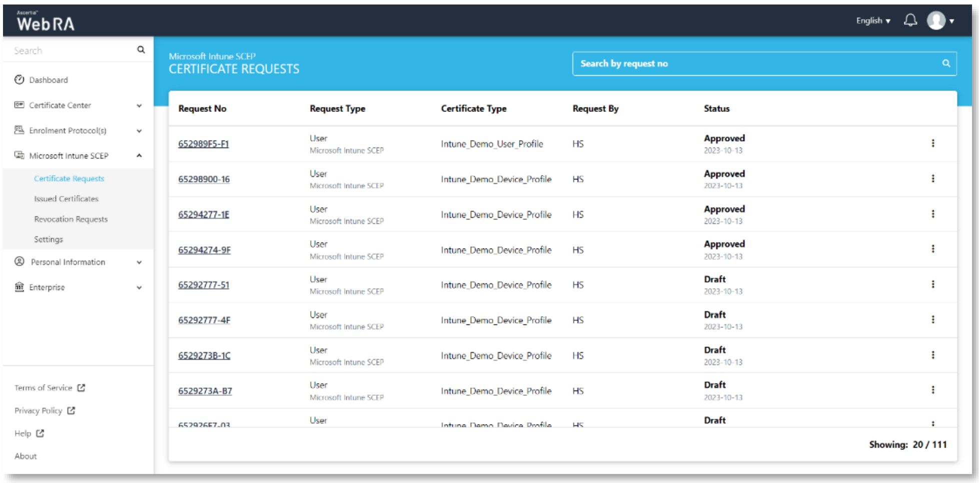
Password * ••••••••••

10/255

✓ Remember Me

2. From the left pane, expand Microsoft Intune SCEP > Create Requests.

This page consists of all the certificate requests including approved, and requests in draft form, due to any limitations from ADSS Web RA.



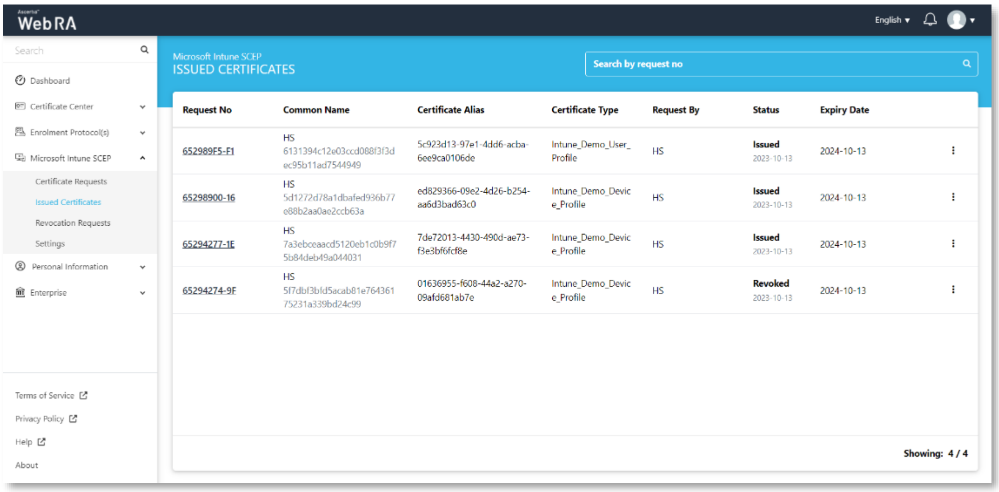
Microsoft Intune SCEP
CERTIFICATE REQUESTS

Search by request no

Request No	Request Type	Certificate Type	Request By	Status
652989F5-F1	User Microsoft Intune SCEP	Intune_Demo_User_Profile	HS	Approved 2023-10-13
65298900-16	User Microsoft Intune SCEP	Intune_Demo_Device_Profile	HS	Approved 2023-10-13
65294277-1E	User Microsoft Intune SCEP	Intune_Demo_Device_Profile	HS	Approved 2023-10-13
65294274-9F	User Microsoft Intune SCEP	Intune_Demo_Device_Profile	HS	Approved 2023-10-13
65292777-51	User Microsoft Intune SCEP	Intune_Demo_Device_Profile	HS	Draft 2023-10-13
65292777-4F	User Microsoft Intune SCEP	Intune_Demo_Device_Profile	HS	Draft 2023-10-13
6529273B-1C	User Microsoft Intune SCEP	Intune_Demo_Device_Profile	HS	Draft 2023-10-13
6529273A-B7	User Microsoft Intune SCEP	Intune_Demo_Device_Profile	HS	Draft 2023-10-13
652926F7-03	User	Intune_Demo_Device_Profile	HS	Draft

Showing: 20 / 111

3. Click Issued Certificates to view all the certificates including issued, revoked, expired, etc.



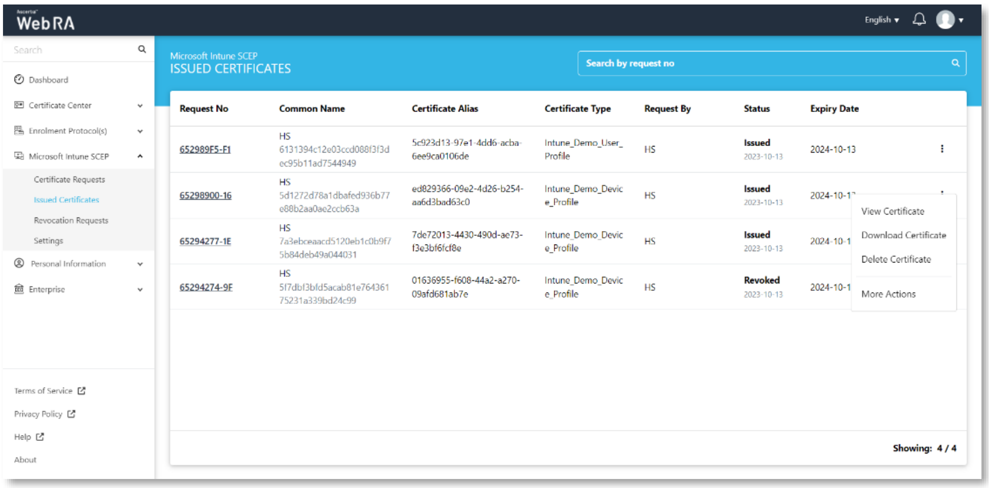
Microsoft Intune SCEP
ISSUED CERTIFICATES

Search by request no

Request No	Common Name	Certificate Alias	Certificate Type	Request By	Status	Expiry Date
652989F5-F1	HS 6131394c12e03ccd088f3f3dec95b11ad7544949	5c923d13-97e1-4dd6-acba-6ee9ca0106de	Intune_Demo_User_Profile	HS	Issued 2023-10-13	2024-10-13
65298900-16	HS 5d1272d78a1dbafed936b77e88b2aa0ae2ccb63a	ed829366-09e2-4d26-b254-aa6d3bad63c0	Intune_Demo_Device_Profile	HS	Issued 2023-10-13	2024-10-13
65294277-1E	HS 7a3ebceaacd5120eb1c0b9f75b84deb49a044031	7de72013-4430-490d-ae73-f3e3bf6fcf8e	Intune_Demo_Device_Profile	HS	Issued 2023-10-13	2024-10-13
65294274-9F	HS 5f7dbf3bfd5acab81e76436175231a339bd24c99	01636955-f608-44a2-a270-09afd681ab7e	Intune_Demo_Device_Profile	HS	Revoked 2023-10-13	2024-10-13

Showing: 4 / 4

4. To revoke a certificate, click ⋮ against a certificate, and then click More Actions.

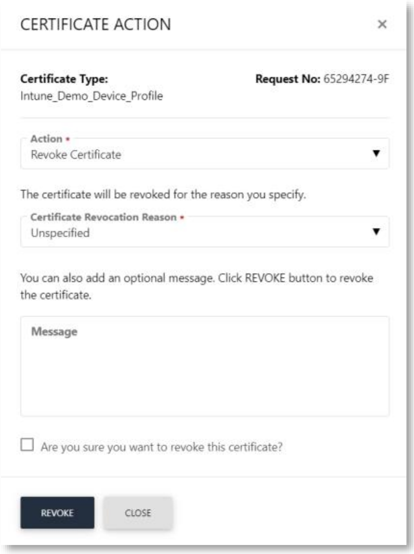


Microsoft Intune SCEP
ISSUED CERTIFICATES

Request No	Common Name	Certificate Alias	Certificate Type	Request By	Status	Expiry Date
652989F5-F1	HS 6131394c12e03ccd088f3f3d ec95b11ad7544949	5c923d13-97e1-4dd6-acba-6ee9ca0106de	Intune_Demo_User_Profile	HS	Issued 2023-10-13	2024-10-13
65298900-16	HS 5d1272d78a1dbafed936b77 e88b2aa0ae2ccb63a	ed829366-09e2-4d26-b254-aa6d3bad63c0	Intune_Demo_Device_Profile	HS	Issued 2023-10-13	2024-10-1
65294277-1E	HS 7a3ebceaacd5120eb1c0b9f7 5b84deb49a044031	7de72013-4430-490d-ae73-f3e3bf6fcf8e	Intune_Demo_Device_Profile	HS	Issued 2023-10-13	2024-10-1
65294274-9F	HS 5f7dbf3bfd5acab81e764361 75231a339bd24c99	01636955-f608-44a2-a270-09afd681ab7e	Intune_Demo_Device_Profile	HS	Revoked 2023-10-13	2024-10-1

Showing: 4 / 4

5. Select Revoke Certificate, and Certificate Revocation Reason and click Revoke.



CERTIFICATE ACTION ×

Certificate Type: Intune_Demo_Device_Profile

Request No: 65294274-9F

Action *
Revoke Certificate ▾

The certificate will be revoked for the reason you specify.

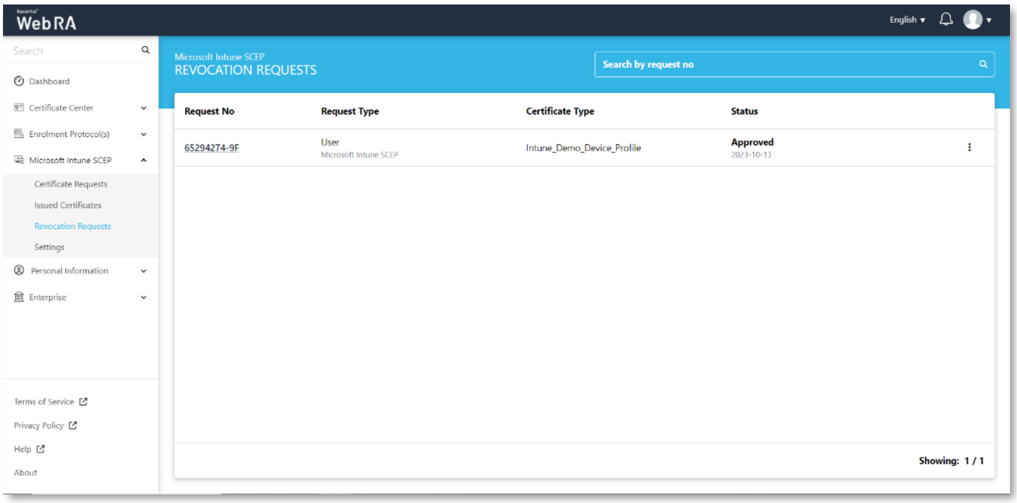
Certificate Revocation Reason *
Unspecified ▾

You can also add an optional message. Click REVOKE button to revoke the certificate.

Message

□ Are you sure you want to revoke this certificate?

6. The certificate will appear in the Revoked Certificates listing.



Microsoft Intune SCEP
REVOCATION REQUESTS

Request No	Request Type	Certificate Type	Status
65294274-9F	User Microsoft Intune SCEP	Intune_Demo_Device_Profile	Approved 2023-10-13

Showing: 1 / 1

8. Troubleshooting

This section lists a few common issues that a user may face while setting up Microsoft Intune SCEP. To ensure a smooth process, you need to ensure the following:

1. If you are already logged in to Ascertia's domain, your Ascertia's account signed up with Microsoft may be logged in automatically. You need to ensure that you either log out from your existing account, and re-login with other credentials or use a different browser.
2. In case you are unable to access Groups in the Microsoft Intune admin center, make sure that you are not connected to Ascertia's network. Switch to a different network to access Groups.
3. While installing the Management Profile in the iOS company portal app, the profiles may not install due to poor network. Ensure that you do not have any connectivity issues while following the instructions mentioned in this document.

For further details, contact us on sales@ascertia.com or visit www.ascertia.com

*** End of Document ***